

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-232776

(43)Date of publication of application : 27.08.1999

(51)Int.Cl. G11B 20/10
G09C 1/00
G11B 20/00
H04L 9/08
H04N 5/91
H04N 5/92
// H04N 7/167

(21)Application number : 10-027572 (71)Applicant : MATSUSHITA ELECTRIC
IND CO LTD

(22)Date of filing : 09.02.1998 (72)Inventor : YAMADA MASAZUMI
IIZUKA HIROYUKI
TAKECHI HIDEAKI
GOTO SHOICHI

(54) VIDEO RECORDING DEVICE AND REPRODUCING DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To make limitations of an effective reproduction period and the number of effective reproduction times of data sure by inputting the whole or a part of correspondence relation information of scrambled video and/or sound data a ciphered scramble key and a ciphered key in which the scramble key is ciphered to a circuit and recording them on a video tape.

SOLUTION: A correspondence relation information generating means 11 generates data and hour information relating AV data which are scrambled with a recording scramble key Kss from a recording scrambling means 7 and a ciphered key Kc in which the recording scramble key Kss is ciphered. A MUX 12 inputs the key Kss from the recording scrambling means 7 the ciphered key Kc from a ciphering means 10 and the data and hour information from the correspondence relation information generating means 11 to record them on a video tape 20. A reproduction descrambling means 17 inputs a key Kss from a key decoding means 16 and descrambles AV data with the key Kss to output descrambled data to a first DMUX 2. Thus the reproducing of the video tape is made possible only for a fixed period after it is recorded.

CLAIMS

[Claim(s)]

[Claim 1] A recording device comprising:

A scramble means which inputs a scramble key for carrying out the scramble of the data of said image and/or a sound and carries out the scramble of the data of said image and/or a sound with the scramble key while inputting data of an image and/or a sound.

An enciphering key generating means which generates an enciphering key for enciphering said scramble key.

A storing means which will eliminate the enciphering key if said enciphering key generating means stores an enciphering key by which it was generated and suits predetermined conditions of the enciphering key after that.

A key encoding means which inputs said enciphering key from said enciphering key generating means and enciphers said scramble key with the enciphering key while inputting a scramble key from said scramble means. An image by which scramble was carried out with said scramble key and/or data of a sound. A correspondence relevant information creating means which generates correspondence relevant information with an enciphering key which enciphered the scramble key. A recording device which inputs all or a part of an image by which scramble was carried out from said scramble means and/or data of a sound, a scramble key enciphered from said key encoding means and correspondence relevant information from said correspondence relevant information creating means and records them on a predetermined recording medium.

[Claim 2] The recording device according to claim 1 after said predetermined conditions is stored [said enciphering key] wherein it means exceeding predetermined time.

[Claim 3] Time into which said scramble means inputted data of said image and/or a sound as said correspondence relevant information. Time to which said scramble means carried out the scramble of the data of said image and/or a sound with said scramble key. Time at which said enciphering key generating means generated said enciphering key. Time in which said storing means stored said enciphering key. The recording device according to claim 1 or 2 being the information matched at time as which said key encoding means enciphered said scramble key with said enciphering key or time at which said recording device recorded data of said image by which scramble was carried out and/or a sound on said predetermined recording medium.

[Claim 4] The recording device according to claim 1 wherein said predetermined conditions mean that the number of times by which said enciphering key was used on the occasion of reproduction of data of said image and/or a sound by which scramble was carried out exceeds the predetermined number of times.

[Claim 5] The recording device according to any one of claims 1 to 4 wherein it has a scramble key generating means which generates said scramble key and said scramble means inputs said scramble key from said scramble key generating

means.

[Claim 6]The recording device according to any one of claims 1 to 4wherein said scramble means inputs said scramble key from a broadcasting station and uses the scramble key.

[Claim 7]Playback equipment comprising:

Said correspondence relevant information according to any one of claims 1 to 6 from the predetermined recording medium according to any one of claims 1 to 6 is inputtedAn enciphering key acquisition means which specifies an image which it is going to reproduceand by which scramble was carried outand/or an enciphering key corresponding to data of a sound based on the correspondence relevant informationand searches and acquires said enciphering key in the storing means according to any one of claims 1 to 6.

While inputting an enciphered scramble key corresponding to data of said image which it is going to reproduce and by which scramble was carried out and/or a sound from said predetermined recording mediumA key encryption decoding means which inputs an enciphering key from said enciphering key acquisition meansand solves encryption of said said enciphered scramble key with the enciphering key. While inputting data of an image by which scramble was carried out from said predetermined recording mediumand/or a soundA releasing scramble means by which a scramble key from said key encryption decoding means is inputtedand the scramble key cancels scramble of data of said image by which scramble was carried outand/or a sound.

[Claim 8]A recording device comprising:

A scramble means which inputs a scramble key for carrying out the scramble of the data of said image and/or a soundand carries out the scramble of the data of said image and/or a sound with the scramble key while inputting data of an image and/or a sound.

An enciphering key generating means which generates an enciphering key for enciphering said scramble key.

A storing means which stores an enciphering key which said enciphering key generating means generated.

A key encoding means which inputs said enciphering key from said enciphering key generating meansand enciphers said scramble key with the enciphering key while inputting a scramble key from said scramble meansAn image by which scramble was carried out with said scramble keyand/or data of a soundA correspondence relevant information creating means which generates correspondence relevant information with an enciphering key which enciphered the scramble keyA recording device which inputs all or a part of an image by which scramble was carried out from said scramble means and/or data of a soundscramble key enciphered from said key encoding meansand correspondence relevant information from said correspondence relevant information creating meansand records them on a predetermined recording medium.

[Claim 9]Time into which said scramble means inputted data of said image and/or a sound as said correspondence relevant informationTime to which said scramble means carried out the scramble of the data of said image and/or a sound with said scramble keyTime at which said enciphering key generating means generated said enciphering keytime in which said storing means stored said enciphering keyThe recording device according to claim 8 being the information matched at time as which said key encoding means enciphered said scramble key with said enciphering keyor time at which said recording device recorded data of said image by which scramble was carried outand/or a sound on said predetermined recording medium.

[Claim 10]The recording device according to claim 8 or 9wherein it has a scramble key generating means which generates said scramble key and said scramble means inputs said scramble key from said scramble key generating means.

[Claim 11]The recording device according to claim 8 or 9wherein said scramble means inputs said scramble key from a broadcasting station and uses the scramble key.

[Claim 12]Playback equipment comprising:

The correspondence relevant information according to any one of claims 8 to 11 from the predetermined recording medium according to any one of claims 8 to 11 is inputtedBased on the correspondence relevant informationan image which it is going to reproduce and by which scramble was carried outand/or an enciphering key corresponding to data of a sound are specifiedAn enciphering key acquisition means which it judges whether the enciphering key suits predetermined conditionstakes out the enciphering key from the storing means according to any one of claims 8 to 11 when agreeingand does not take out the enciphering key from said storing means when not agreeing.

While inputting an enciphered scramble key corresponding to data of said image which it is going to reproduce and by which scramble was carried out and/or a sound from said predetermined recording mediumA key encryption decoding means which inputs an enciphering key from said enciphering key acquisition meansand solves encryption of said said enciphered scramble key with the enciphering key. While inputting data of an image by which scramble was carried out from said predetermined recording mediumand/or a soundA releasing scramble means by which a scramble key from said key encryption decoding means is inputtedand the scramble key cancels scramble of data of said image by which scramble was carried outand/or a sound.

[Claim 13]The playback equipment according to claim 12 after said predetermined conditions is stored [said enciphering key] in the storing means according to any one of claims 8 to 11wherein it means exceeding predetermined time.

[Claim 14]The playback equipment according to claim 12wherein said predetermined conditions mean that the number of times by which said enciphering key was used on the occasion of reproduction of data of said image and/or a sound by which scramble was carried out exceeds the predetermined number of times.

[Claim 15]A recording device comprising:

A scramble key generating means which generates a scramble key for carrying out the scramble of the data of an image and/or a sound.

A storing means which will eliminate the scramble key if said scramble key generating means stores a scramble key by which it was generated and suits predetermined conditions of the scramble key after that.

A scramble means which inputs a scramble key from said scramble key generating means and carries out the scramble of the data of said image and/or a sound with the scramble key while inputting data of said image and/or a sound.

An image by which scramble was carried out with said scramble key and/or data of a soundA correspondence relevant information creating means which generates correspondence relevant information with the scramble keyA recording device which inputs an image by which scramble was carried out from said scramble means and/or data of a sound and all or a part of correspondence relevant information from said correspondence relevant information creating means and records them on a predetermined recording medium.

[Claim 16]The recording device according to claim 15 after said predetermined conditions is stored [said scramble key]wherein it means exceeding predetermined time.

[Claim 17]Time into which said scramble means inputted data of said image and/or a sound as said correspondence relevant informationTime to which said scramble means carried out the scramble of the data of said image and/or a sound with said scramble keyTime at which said scramble key generating means generated said scramble keytime in which said storing means stored said scramble keyOr the recording device according to claim 15 or 16wherein said recording device is the information matched at time which recorded data of said image by which scramble was carried out and/or a sound on said predetermined recording medium.

[Claim 18]The recording device according to claim 15wherein said predetermined conditions mean that the number of times by which said enciphering key was used on the occasion of reproduction of data of said image and/or a sound by which scramble was carried out exceeds the predetermined number of times.

[Claim 19]Playback equipment comprising:

The correspondence relevant information according to any one of claims 15 to 18 from the predetermined recording medium according to any one of claims 15 to 18 is inputtedA scramble key acquisition means which specifies an image which it is going to reproduce and by which scramble was carried out and/or a scramble key corresponding to data of a sound based on the correspondence relevant information and searches and acquires said scramble key in the storing means according to any one of claims 15 to 18.

While inputting data of said image from said predetermined recording medium which it is going to reproduce and by which scramble was carried out said image corresponding to data of a sound by which scramble was carried out and/or a soundA releasing scramble means by which a scramble key from said scramble key

acquisition means is inputted and the scramble key cancels scramble of data of said image by which scramble was carried out and/or a sound.

[Claim 20] A recording device comprising:

A scramble key generating means which generates a scramble key for carrying out the scramble of the data of an image and/or a sound.

A storing means which stores a scramble key which said scramble key generating means generated.

A scramble means which inputs a scramble key from said scramble key generating means and carries out the scramble of the data of said image and/or a sound with the scramble key while inputting data of said image and/or a sound.

An image by which scramble was carried out with said scramble key and/or data of a sound A correspondence relevant information creating means which generates correspondence relevant information with the scramble key A recording device which inputs an image by which scramble was carried out from said scramble means and/or data of a sound and all or a part of correspondence relevant information from said correspondence relevant information creating means and records them on a predetermined recording medium.

[Claim 21] Time into which said scramble means inputted data of said image and/or a sound as said correspondence relevant information Time to which said scramble means carried out the scramble of the data of said image and/or a sound with said scramble key Time at which said scramble key generating means generated said scramble key time in which said storing means stored said scramble key Or the recording device according to claim 20 wherein said recording device is the information matched at time which recorded data of said image by which scramble was carried out and/or a sound on said predetermined recording medium.

[Claim 22] Playback equipment comprising:

The correspondence relevant information according to claim 20 or 21 from the predetermined recording medium according to claim 20 or 21 is inputted Based on the correspondence relevant information an image which it is going to reproduce and by which scramble was carried out and/or a scramble key corresponding to data of a sound are specified A scramble key acquisition means which it judges whether the scramble key suits predetermined condition stakes out the scramble key from the storing means according to claim 20 or 21 when agreeing and does not take out the scramble key from said storing means when not agreeing.

While inputting data of said image from said predetermined recording medium which it is going to reproduce and by which scramble was carried out an image corresponding to data of a sound by which scramble was carried out and/or a sound A releasing scramble means by which a scramble key from said scramble key acquisition means is inputted and the scramble key cancels scramble of data of said image by which scramble was carried out and/or a sound.

[Claim 23] The playback equipment according to claim 22 after said predetermined

conditions is stored [said scramble key] in the storing means according to claim 20 or 21 wherein it means exceeding predetermined time.

[Claim 24] The playback equipment according to claim 22 wherein said predetermined conditions mean that the number of times by which said scramble key was used on the occasion of reproduction of data of said image and/or a sound by which scramble was carried out exceeds the predetermined number of times.

[Claim 25] Said recording device data of an image by which scramble was carried out from said scramble means and/or a sound Either of claims 1-6 having a charging means which imposes fee collection to record of said data when recording on said predetermined recording medium Or either of claims 8-11 either of claims 15-18 or the recording device according to any one of claims 20 to 21.

[Claim 26] Either of claims 1-6 wherein said predetermined recording medium is videotape either of claims 8-11 either of claims 15-18 or the recording device according to any one of claims 20 to 21.

[Claim 27] Either of claims 1-6 wherein said predetermined recording medium is a hard disk either of claims 8-11 either of claims 15-18 or the recording device according to any one of claims 20 to 21.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the recording device which records the data of the image and/or sound to which the period about playback and the number of times were restricted by copyright etc. and the playback equipment which plays the data of the image and/or a sound.

[0002]

[Description of the Prior Art] Now AV information which has been the targets of copyright protections such as a movie and music is stored in videotape etc. The user can appreciate a movie music etc. when only a predetermined period when it says that such videotape etc. are one week through the rental store which lends out for pay borrows videotape etc. and plays it.

[0003] On the other hand apart from the system of a rental of the videotape etc. which were mentioned above from progress of digital art and encoding technology etc. Programs such as a movie from a broadcasting station and music are inputted via a communications satellite the scramble of the program is carried out it records on videotape etc. and the following are considered as recording playback equipment to play.

[0004] The block diagram of such conventional recording playback equipment is shown in drawing 7.

[0005] The receiving demodulation means 1 The picture image data of DEJITARU of satellite broadcastingsound data Inputting EMM (individual information) ECM

(program information) and the enciphered broadcast scramble key K_s 1st DMUX2 separates the picture image data the sound data EMM ECM and the broadcast scramble key K_s from the receiving demodulation means 1. And the EMM decoding means 3 inputs the user ID key K_m decodes EMM with the user ID key K_m and generates the work key K_w while it inputs EMM from the 1DMUX2. The ECM decoding means 4 inputs ECM and the enciphered broadcast scramble key K_s from the 1DMUX2 decodes ECM with the work key K_w and restores the enciphered broadcast scramble key K_s while it inputs the work key K_w from the EMM decoding means 3.

[0006] Then the broadcast descrambling means 5 inputs the AV information by which scramble was carried out from the 1DMUX2 is the broadcast scramble key K_s and descrambles the AV information by which scramble was carried out while it inputs the broadcast scramble key K_s from the ECM decoding means 4. And the broadcast descrambling means 5 is outputted to the record scramble means 7 when outputting the descrambled AV information to 1st DMUX2 when displaying AV information on the display 21 directly in real time and making AV information record on the videotape 20.

[0007] When the broadcast descrambling means 5 outputs AV information to 1st DMUX2 1st DMUX2 divides the AV information from the broadcast descrambling means 5 into picture image data and sound data it outputs picture image data to the video decoder 18 and outputs sound data to the sound decoder 19. and the video decoder 18 and the sound decoder 19 -- each decodes the picture image data or sound data from the 1DMUX2 and the display 21 displays an image and outputs a sound.

[0008] On the other hand when the broadcast descrambling means 5 outputs AV information to the record scramble means 7 the record scramble means 7 While inputting the AV information from the broadcast descrambling means 5 the record scramble key K_{ss} from the 1st key generating means 6 is inputted and the scramble of the AV information is carried out with the record scramble key K_{ss} . AV information by which scramble was carried out with the record scramble key K_{ss} is set to K_{ss} (AV information).

[0009] With it generate the 2nd key generating means 8 and the enciphering key K_c for enciphering the record scramble key K_{ss} the key encoding means 10 While inputting the record scramble key K_{ss} from the 1st key generating means 6 the enciphering key K_c from the 2nd key generating means 8 is inputted and the record scramble key K_{ss} is enciphered with the enciphering key K_c . The record scramble key K_{ss} enciphered by the enciphering key K_c is set to K_c (K_{ss}).

[0010] And MUX12 inputs K_{ss} (AV information) from the record scramble means 7 and K_c (K_{ss}) from the key encoding means 10 and records them on the videotape 20.

[0011] When playing K_{ss} (AV information) recorded on the videotape 20 first 2nd DMUX13 inputs K_{ss} (AV information) from the videotape 20 and K_c (K_{ss}) and dissociates. And the key decoding means 16 inputs the enciphering key K_c from the 2nd key generating means 8 decodes K_c (K_{ss}) with the enciphering key K_c and

restores the record scramble key Kss while it inputs Kc (Kss) from the 2DMUX13. While the reproduction descrambling means 17 inputs Kss (AV information) from the 2DMUX13. The record scramble key Kss from the key decoding means 16 is inputted. Kss (AV information) is descrambled with the record scramble key Kss and the descrambled AV information is outputted to 1st DMUX2.

[0012] Finally the AV information outputted to 1st DMUX2 is displayed as an image on the display 21 as well as the graphic display of the display 21 and the sound output in real time and is outputted as a sound.

[0013]

[Problem(s) to be Solved by the Invention] By the way also in the future multi-channel digital-broadcasting age a user goes to a rental store each time the point that videotape etc. must be borrowed etc. take time and effort as usual for a user and the system of a rental of the videotape etc. which were mentioned above is inconvenience.

[0014] Once it records [the conventional recording playback equipment mentioned above] AV information on the videotape 20 if only it will use the enciphering key Kc from the 2nd key generating means 8 the AV information. It is reproduced any number of times and outputted as an image and/or a sound on the display 21 again always. Thus in conventional recording playback equipment it will be said that there is no restriction between the effective regeneration phases of the AV information which has been the target of copyright protections such as a movie and music and in effective reproduction frequency. For example if recorded on a recording medium with the recording playback equipment which does not have restriction about a reproductive period or number of times which the AV information which has special value mentioned above like the movie immediately after theater televising worth of the AV information will be reduced by half. That is the broadcasting station cannot broadcast in comfort the AV information which has such special value.

[0015] This invention such conventional recording playback equipment. If AV information is recorded on a recording medium the technical problem that neither during the effective regeneration phase of the AV information nor restriction of effective reproduction frequency is protected will be taken into consideration. AV information is recorded on a recording medium and it aims at providing the recording device and playback equipment which observe during the effective regeneration phase of the AV information and restriction of effective reproduction frequency.

[0016]

[Means for Solving the Problem] A recording device this invention of claim 1 is characterized by that comprises the following.

A scramble means which inputs a scramble key for carrying out the scramble of the data of said image and/or a sound and carries out the scramble of the data of said image and/or a sound with the scramble key while inputting data of an image and/or a sound.

An enciphering key generating means which generates an enciphering key for

enciphering said scramble key.

A storing means which will eliminate the enciphering key if said enciphering key generating means stores an enciphering key by which it was generated and suits predetermined conditions of the enciphering key after that.

A key encoding means which inputs said enciphering key from said enciphering key generating means and enciphers said scramble key with the enciphering key while inputting a scramble key from said scramble means. An image by which scramble was carried out with said scramble key and/or data of a sound. A correspondence relevant information creating means which generates correspondence relevant information with an enciphering key which enciphered the scramble key. A recording device which inputs all or a part of an image by which scramble was carried out from said scramble means and/or data of a sound. A scramble key enciphered from said key encoding means and correspondence relevant information from said correspondence relevant information creating means and records them on a predetermined recording medium.

[0017] Playback equipment this invention of claim 7 is characterized by that comprises the following.

Said correspondence relevant information according to any one of claims 1 to 6 from the predetermined recording medium according to any one of claims 1 to 6 is inputted. An enciphering key acquisition means which specifies an image which it is going to reproduce and by which scramble was carried out and/or an enciphering key corresponding to data of a sound based on the correspondence relevant information and searches and acquires said enciphering key in the storing means according to any one of claims 1 to 6.

While inputting an enciphered scramble key corresponding to data of said image which it is going to reproduce and by which scramble was carried out and/or a sound from said predetermined recording medium. A key encryption decoding means which inputs an enciphering key from said enciphering key acquisition means and solves encryption of said said enciphered scramble key with the enciphering key. While inputting data of an image by which scramble was carried out from said predetermined recording medium and/or a sound. A releasing scramble means by which a scramble key from said key encryption decoding means is inputted and the scramble key cancels scramble of data of said image by which scramble was carried out and/or a sound.

[0018] A recording device this invention of claim 8 is characterized by that comprises the following.

A scramble means which inputs a scramble key for carrying out the scramble of the data of said image and/or a sound and carries out the scramble of the data of said image and/or a sound with the scramble key while inputting data of an image and/or a sound.

An enciphering key generating means which generates an enciphering key for enciphering said scramble key.

A storing means which stores an enciphering key which said enciphering key generating means generated.

A key encoding means which inputs said enciphering key from said enciphering key generating means and enciphers said scramble key with the enciphering key while inputting a scramble key from said scramble means. An image by which scramble was carried out with said scramble key and/or data of a sound. A correspondence relevant information creating means which generates correspondence relevant information with an enciphering key which enciphered the scramble key. A recording device which inputs all or a part of an image by which scramble was carried out from said scramble means and/or data of a sound. A scramble key enciphered from said key encoding means and correspondence relevant information from said correspondence relevant information creating means and records them on a predetermined recording medium.

[0019] Playback equipment this invention of claim 12 is characterized by that comprises the following.

The correspondence relevant information according to any one of claims 8 to 11 from the predetermined recording medium according to any one of claims 8 to 11 is inputted. Based on the correspondence relevant information, an image which it is going to reproduce and by which scramble was carried out and/or an enciphering key corresponding to data of a sound are specified. An enciphering key acquisition means which it judges whether the enciphering key suits predetermined conditions, takes out the enciphering key from the storing means according to any one of claims 8 to 11 when agreeing and does not take out the enciphering key from said storing means when not agreeing.

While inputting an enciphered scramble key corresponding to data of said image which it is going to reproduce and by which scramble was carried out and/or a sound from said predetermined recording medium, a key encryption decoding means which inputs an enciphering key from said enciphering key acquisition means and solves encryption of said said enciphered scramble key with the enciphering key. While inputting data of an image by which scramble was carried out from said predetermined recording medium and/or a sound, a releasing scramble means by which a scramble key from said key encryption decoding means is inputted and the scramble key cancels scramble of data of said image by which scramble was carried out and/or a sound.

[0020] A recording device this invention of claim 15 is characterized by that comprises the following.

A scramble key generating means which generates a scramble key for carrying out the scramble of the data of an image and/or a sound.

A storing means which will eliminate the scramble key if said scramble key generating means stores a scramble key by which it was generated and suits predetermined conditions of the scramble key after that.

A scramble means which inputs a scramble key from said scramble key generating

means and carries out the scramble of the data of said image and/or a sound with the scramble key while inputting data of said image and/or a sound.

An image by which scramble was carried out with said scramble key and/or data of a sound
A correspondence relevant information creating means which generates correspondence relevant information with the scramble key
A recording device which inputs an image by which scramble was carried out from said scramble means and/or data of a sound and all or a part of correspondence relevant information from said correspondence relevant information creating means and records them on a predetermined recording medium.

[0021] Playback equipment this invention of claim 19 is characterized by that comprises the following.

The correspondence relevant information according to any one of claims 15 to 18 from the predetermined recording medium according to any one of claims 15 to 18 is inputted
A scramble key acquisition means which specifies an image which it is going to reproduce and by which scramble was carried out and/or a scramble key corresponding to data of a sound based on the correspondence relevant information and searches and acquires said scramble key in the storing means according to any one of claims 15 to 18.

While inputting data of said image from said predetermined recording medium which it is going to reproduce and by which scramble was carried out said image corresponding to data of a sound by which scramble was carried out and/or a sound
A releasing scramble means by which a scramble key from said scramble key acquisition means is inputted and the scramble key cancels scramble of data of said image by which scramble was carried out and/or a sound.

[0022] A recording device this invention of claim 20 is characterized by that comprises the following.

A scramble key generating means which generates a scramble key for carrying out the scramble of the data of an image and/or a sound.

A storing means which stores a scramble key which said scramble key generating means generated.

A scramble means which inputs a scramble key from said scramble key generating means and carries out the scramble of the data of said image and/or a sound with the scramble key while inputting data of said image and/or a sound.

An image by which scramble was carried out with said scramble key and/or data of a sound
A correspondence relevant information creating means which generates correspondence relevant information with the scramble key
A recording device which inputs an image by which scramble was carried out from said scramble means and/or data of a sound and all or a part of correspondence relevant information from said correspondence relevant information creating means and records them on a predetermined recording medium.

[0023] Playback equipment this invention of claim 22 is characterized by that

comprises the following.

The correspondence relevant information according to claim 20 or 21 from the predetermined recording medium according to claim 20 or 21 is inputted. Based on the correspondence relevant information, an image which it is going to reproduce and by which scramble was carried out and/or a scramble key corresponding to data of a sound are specified. A scramble key acquisition means which it judges whether the scramble key suits predetermined conditions takes out the scramble key from the storing means according to claim 20 or 21 when agreeing and does not take out the scramble key from said storing means when not agreeing. While inputting data of said image from said predetermined recording medium which it is going to reproduce and by which scramble was carried out, an image corresponding to data of a sound by which scramble was carried out and/or a sound. A releasing scramble means by which a scramble key from said scramble key acquisition means is inputted and the scramble key cancels scramble of data of said image by which scramble was carried out and/or a sound.

[0024]

[Embodiment of the Invention] Below an embodiment of the invention is described with reference to drawings.

[0025] (Embodiment 1) The composition of the recording device of the embodiment of the invention 1 and playback equipment is described first.

[0026] The block diagram of the recording device of the embodiment of the invention 1 and playback equipment is shown in drawing 1. The recording device of ***** comprises:

The 1st key generating means 6.

Record scramble means 7.

The 2nd key generating means 8.

Kc FIFO 9, the key encoding means 10, the correspondence relevant information creating means 11 and MUX 12.

The playback equipment of ***** comprises:

The 2D MUX 13.

Enciphering key acquisition means 14.

Kc latch means 15.

The key decoding means 16 and the reproduction descrambling means 17.

The receiving demodulation means 1, 1st DMUX 2, the EMM decoding means 3, the ECM decoding means 4, the broadcast descrambling means 5, the video decoder 18 and the sound decoder 19 are also displayed on drawing 1. The videotape 20 as a recording medium and an image are displayed and the display 21 which outputs a sound is also displayed.

[0027] The receiving demodulation means 1 is a means to input the picture image data, the sound data, EMM (individual information), ECM (program information) and the enciphered broadcast scramble key Ks of DEJITARU from a broadcasting station via a communications satellite and to operate those all or some signal wave forms orthopedically.

[0028]The picture image data and sound data which the receiving demodulation means 1 inputs are the data by which scramble was carried out with the broadcast scramble key Ks. Belowwhen you mean both picture image data and sound data let picture image data and sound data be AV information.

[0029]EMM (individual information) which the receiving demodulation means 1 inputs is information which is needed when generating a key called the work key Kw explained later.

[0030]ECM (program information) which the receiving demodulation means 1 inputs is information which is needed when restoring the enciphered broadcast scramble key Ks.

[0031]Nowwhile 1st DMUX2 is a means to separate the picture image data and sound data by which waveform shaping was carried outEMMECMand the enciphered broadcast scramble key Ks of the receiving demodulation means 1It is a means to separate the picture image data and sound data of the broadcast descrambling means 5 which were descrambled. 1st DMUX2 is also a means to separate the picture image data and sound data from the reproduction descrambling means 17.

[0032]The EMM decoding means 3 is a means to input EMM from the 1DMUX2to decode EMM with the user ID key Km and to generate the work key Kw while inputting the user ID key Km.

[0033]The ECM decoding means 4 is a means to input ECM and the enciphered broadcast scramble key Ks from the 1DMUX2to decode ECM with the work key Kw and to restore the broadcast scramble key Ks while inputting the work key Kw from the EMM decoding means 3.

[0034]The broadcast descrambling means 5 inputs the AV information by which scramble was carried out from the 1DMUX2is the broadcast scramble key Ks and is a means to descramble the AV information by which scramble was carried out while it inputs the broadcast scramble key Ks from the ECM decoding means 4.

[0035]The 1st key generating means 6 is a means to generate the record scramble key Kss for carrying out the scramble of the AV information descrambled by the broadcast descrambling means 5 again.

[0036]The record scramble means 7 is a means which inputs the record scramble key Kss from the 1st key generating means 6 and carries out the scramble of the AV information with the record scramble key Kss while inputting the AV information from the broadcast descrambling means 5. BelowAV information by which scramble was carried out with the record scramble key Kss is set to Kss (AV information).

[0037]The 2nd key generating means 8 is a means to generate the enciphering key Kc for enciphering the record scramble key Kss which the 1st key generating means 6 generated. The 2nd key generating means 8 shall generate the enciphering key Kc different every day and makes these different **** Kc Kc1Kc2Kc3 and -- respectively. enciphering key Kc1Kc2Kc3 and -- each presupposes that it is what is discarded in one week.

[0038]While KcFIFO9 is a means to input and store enciphering key Kc1 from the

2nd key generating means 8Kc2Kc3and --It is a means has a timer and discard the enciphering key Kc which passed for one week after the input using the timer to have a first in farce out function.

[0039]The key encoding means 10 is a means to input the enciphering key Kc from KcFIFO9 and to encipher the record scramble key Kss with the enciphering key Kc while inputting the record scramble key Kss from the 1st key generating means 6. Belowthe record scramble key Kss enciphered by the enciphering key Kc is set to Kc (Kss).

[0040]The correspondence relevant information creating means 11 is a means to generate the information on time that enciphering key Kc4 was generatedas information for matching the AV information by which scramble was carried out with the record scramble key Kssand the enciphering key Kc which enciphered the record scramble key Kss.

[0041]MUX12 is a means to input Kss (AV information) from the record scramble means 7Kc (Kss) from the key encoding means 10and the date information from the correspondence relevant information creating means 11and to record them on the videotape 20.

[0042]2nd DMUX13 is a means to input Kss (AV information)Kc (Kss)and date information which were recorded on the videotape 20and to separate them.

[0043]The enciphering key acquisition means 14 is a means to input the date information from the 2DMUX13to specify the enciphering key Kc corresponding to Kss (AV information) which it is going to reproduce based on the date informationand to acquire the specified enciphering key Kc out of KcFIFO9.

[0044]The Kc latch means 15 is a means to input and latch the enciphering key Kc from the enciphering key acquisition means 14and to output to the key decoding means 16.

[0045]The key decoding means 16 is a means to input the enciphering key Kc from the Kc latch means 15to decode Kc (Kss) with the enciphering key Kcand to restore the record scramble key Kss while inputting Kc (Kss) from the 2DMUX13.

[0046]The reproduction descrambling means 17 is a means to input the record scramble key Kss from the key decoding means 16and to descramble Kss (AV information) with the record scramble key Kss while inputting Kss (AV information) from the 2DMUX13.

[0047]The video decoder 18 is a means to decode the picture image data from the 1DMUX2.

[0048]The sound decoder 19 is a means to decode the sound data from the 1DMUX2.

[0049]This invention of claim 1It was considered as the scramble meansand used the 2nd key generating means 8 as the record scramble means 7 and an enciphering key generating meansthe correspondence relevant information creating means 11 was used as a storing meansand MUX12 was used as a recording device as the key encoding means 10 and a correspondence relevant information creating means as KcFIFO9 and a key encoding means. The 1st key generating means 6 was used by this embodiment as a scramble key generating

means of this invention of claim 6. The reproduction descrambling means 17 was used as the key decoding means 16 and a releasing scramble means as the enciphering key acquisition means 14 and a key encryption decoding means as an enciphering key acquisition means of this invention of claim 7.

[0050]Next operation of the recording device of such an embodiment of the invention 1 is described.

[0051]The receiving demodulation means 1 First the picture image data of DEJITARU from a broadcasting station Sound data EMM (individual information) ECM (program information) and the enciphered broadcast scramble key Ks are inputted Disorder of the signal wave form of picture image data and sound data is operated orthopedically and picture image data sound data EMMECM and the enciphered broadcast scramble key Ks are outputted to 1st DMUX2.

[0052]Then 1st DMUX2 inputs the picture image data the sound data EMMECM and the broadcast scramble key Ks from the receiving demodulation means 1 it dissociates and outputs picture image data and sound data (AV information) to the broadcast descrambling means 5. EMM is outputted to the EMM decoding means 3 and ECM and the enciphered broadcast scramble key Ks are outputted to the ECM decoding means 4.

[0053]Next it inputs EMM from the 1DMUX2 the EMM decoding means 3 decodes EMM with the user ID key Km generates the work key Kw and outputs it to the ECM decoding means 4 while it inputs the user ID key Km.

[0054]While the ECM decoding means 4 inputs the work key Kw from the EMM decoding means 3 ECM and the enciphered broadcast scramble key Ks from the 1DMUX2 are inputted ECM is decoded with the work key Kw encryption of the enciphered broadcast scramble key Ks is restored and it outputs to the broadcast descrambling means 5. And the broadcast descrambling means 5 inputs the AV information by which scramble was carried out from the 1DMUX2 is the broadcast scramble key Ks and descrambles the AV information by which scramble was carried out while it inputs the broadcast scramble key Ks from the ECM decoding means 4. And the broadcast descrambling means 5 outputs the descrambled AV information to the 1DMUX2 or the record scramble means 7. The broadcast descrambling means 5 is outputted to 1st DMUX2 when displaying AV information on the display 21 directly in real time and when making AV information record on the videotape 20 it is outputted to the record scramble means 7. However the AV information recorded on the videotape 20 is not AV information as it is but the data by which scramble was carried out again from the broadcast descrambling means 5.

[0055]First the case where the broadcast descrambling means 5 outputs AV information to 1st DMUX2 is explained.

[0056]In that case 1st DMUX2 carries out an AV information input from the broadcast descrambling means 5 divides it into picture image data and sound data outputs picture image data to the video decoder 18 and outputs sound data to the sound decoder 19. then the video decoder 18 and the sound decoder 19 -- each decodes the picture image data or sound data from the 1DMUX2 and outputs

it to the display 21. And the display 21 displays an image and outputs a sound.

[0057]Next the case where the broadcast descrambling means 5 outputs AV information to the record scramble means 7 is explained. That is as mentioned above it is a case where AV information is recorded on the videotape 20.

[0058]First the record scramble means 7 inputs the AV information descrambled from the broadcast descrambling means 5.

[0059]And the 1st key generating means 6 generates the record scramble key Kss for carrying out the scramble of the AV information which the record scramble means 7 inputs and outputs it to the record scramble means 7 and the key encoding means 10.

[0060]Next the record scramble means 7 inputs the record scramble key Kss from the 1st key generating means 6 and carries out the scramble of the AV information with the record scramble key Kss. That is Kss (AV information) is generated. And Kss (AV information) is outputted to the correspondence relevant information creating means 11 and MUX 12.

[0061]On the other hand the 2nd key generating means 8 generates the enciphering key Kc for enciphering the record scramble key Kss which the 1st key generating means 6 generated. The enciphering keys Kc which the 2nd key generating means 8 generates shall differ every day. As it supposes here that it is the day of the following explanation when the recording device begins to operate for convenience on January 1 1998 it supposes that it is today which it is at the record time on January 4 1998 three days after the day and it is shown in the enciphering key Kc list (a) of drawing 2 Kc2—the enciphering key Kc generated on January 4 are set to Kc4 for the enciphering key Kc generated in the enciphering key Kc generated on January 1 on Kc January [1 or]2. The enciphering key Kc shall be generated in a similar manner hereafter. As long as there is no notice operation of the recording device on January 4 is explained hereafter.

[0062]Now as shown in the list of drawing 2 (a) from January 1 every one enciphering key Kc is already inputted from the 2nd key generating means 8 and Kc FIFO 9 stores it every day it will store enciphering key Kc1 Kc2 and Kc3 by January 3 and inputs and stores Kc4 on January 4 today. The storing is performed so that the newest enciphering key Kc may always come to the ranking of the top of the list of drawing 2 (a) and an old thing is performed so that ranking may be lowered one by one. Kc FIFO 9 discards enciphering key Kc1 stored Kc2 and —after passing for one week since each storing. For example when it becomes as [show / in the list of drawing 2 (b)] on January 9 an enciphering key called Kc1 and Kc2 will be discarded and Kc FIFO 9 will store seven enciphering keys in Kc9 Kc8—order of Kc4 and Kc3. That is the number of the enciphering keys Kc which Kc FIFO 9 stores is to 7.

[0063]Next via Kc FIFO 9 the key encoding means 10 inputs enciphering key Kc4 generated on January 4 it is whose 2nd key generating means 8 at the record time and enciphers the record scramble key Kss by the enciphering key Kc4 while it inputs the record scramble key Kss from the 1st key generating means 6. That is Kc4 (Kss) is generated.

[0064]The correspondence relevant information creating means 11 And Kss (AV information) from the record scramble means 7Kc4 (Kss) from the key encoding means 10 is inputted and the information on time that the enciphering key Kc4 was generated is generated as information for matching the enciphering key Kc4 and the AV information by which scramble was carried out with the record scramble key Kss enciphered by the enciphering key Kc4. That is the date information of January 4 is generated.

[0065]Then MUX12 inputs the date information of Kss (AV information) from the record scramble means 7Kc4 (Kss) from the key encoding means 10 and January 4 from the correspondence relevant information creating means 11 makes them 1 set and records them on the videotape 20.

[0066]Thus Kcn (Kss) corresponding to the enciphering key Kcn (n= 12--) generated on that day Kss (AV information) and the date information of the day will be 1 set and are recorded on the videotape 20 every day.

[0067]Next operation of the playback equipment of the embodiment of the invention 1 is described.

[0068]That is the case where Kss (AV information) recorded on the videotape 20 by the recording device is played is explained.

[0069]Suppose that it is the day of the following explanation when playback equipment plays Kss (AV information) of the videotape 20 for convenience on January 9. And playback equipment shall play Kss (AV information) recorded on the videotape 20 on January 1 and Kss (AV information) recorded on the videotape 20 on January 3.

[0070]The case where first playback equipment tends to play Kss (AV information) recorded on the videotape 20 on January 1 is explained.

[0071]First 2nd DMUX13 inputs Kss (AV information) recorded on January 1 from the videotape 20 Kc1 (Kss) and the date information of January 1 separates them and outputs the date information of January 1 to the enciphering key acquisition means 14.

[0072]And the enciphering key acquisition means 14 searches enciphering key Kc1 out of the list of drawing 2 (b) which inputs the date information of the January 1 and specifies enciphering key Kc1 based on the date information and KcFIFO9 stores. However since the enciphering key Kc1 has passed one week or more since generating it is discarded by KcFIFO9 and does not exist in the list of drawing 2 (b). Therefore the enciphering key acquisition means 14 cannot acquire enciphering key Kc1. . As a result it is necessary to descramble the reproduction descrambling means 17 using the enciphering key Kc1 indirectly. Even if it becomes impossible to descramble Kss (AV information) recorded on January 1 and the AV information is outputted to the display 21 since a decipherment is impossible the display 21 cannot output the original image and sound of AV information.

[0073]Next the case where playback equipment tends to play Kss (AV information) recorded on the videotape 20 on January 3 is explained.

[0074]First 2nd DMUX13 inputs Kss (AV information) recorded on January 3 from the videotape 20 Kc3 (Kss) and the date information of January 3 separates

them and outputs the date information of January 3 to the enciphering key acquisition means 14.

[0075] Next the enciphering key acquisition means 14 inputs the date information of the January 3. Based on the date information, enciphering key Kc3 is searched out of the list of drawing 2 (b) which specifies enciphering key Kc3 and KcFIFO9 stores the enciphering key Kc3 and it is outputted to the Kc latch means 15.

[0076] Then the Kc latch means 15 inputs enciphering key Kc3 and outputs it to the key decoding means 16. 2nd DMUX13 outputs Kc3 (Kss) to the key decoding means 16.

[0077] And while the key decoding means 16 inputs Kc3 (Kss) from the 2nd DMUX13, enciphering key Kc3 from the Kc latch means 15 is inputted. Kc3 (Kss) is decoded by the enciphering key Kc3, the record scramble key Kss is restored, and the record scramble key Kss is outputted to the reproduction descrambling means 17. 2nd DMUX13 outputs Kss (AV information) to the key decoding means 16.

[0078] Next while the reproduction descrambling means 17 inputs Kss (AV information) from the 2nd DMUX13, the record scramble key Kss from the key decoding means 16 is inputted. Kss (AV information) is descrambled with the record scramble key Kss, and the descrambled AV information is outputted to 1st DMUX2.

[0079] And 1st DMUX2 inputs the AV information from the reproduction descrambling means 17, divides it into picture image data and sound data, outputs picture image data to the video decoder 18, and outputs sound data to the sound decoder 19. Then the video decoder 18 and the sound decoder 19 — each decodes the picture image data or sound data from the 1st DMUX2 and outputs it to the display 21. And the display 21 displays an image and outputs a sound.

[0080] Thus, unless each Kss (AV information) recorded on the videotape 20 has been less than one week since it was recorded, it is not eventually played as an original image and sound.

[0081] Although each Kss (AV information) recorded on the videotape 20 presupposes that it will be played if it has been less than one week since it was recorded in Embodiment 1 mentioned above, if not restriction of a period such as less than one week, but the reproduction frequency of each Kss (AV information) is restricted, for example like 1 time or 3 times, and it is not in the restriction, reproduction frequency, it is good though not reproduced. That is as shown in drawing 3, the playback equipment of this invention is provided with the counter 22. When reproduction frequency which the counter 22 checks the reproduction frequency of each Kss (AV information), for example it says is 1 time and 3 times, and which was restricted is become, it is good though KcFIFO9 discards the enciphering key Kc corresponding to the Kss (AV information). It is good though restriction of a period and restriction of reproduction frequency such as less than one week mentioned above are used together.

[0082] In Embodiment 1 mentioned above, KcFIFO9 presupposes that it discards after one week goes through the stored enciphering key Kc.

However, KcFIFO9 without discarding even if one week goes through the stored

enciphering key KcIt is judged whether the day when it keeps stored on and the enciphering key acquisition means 14 tends to reproduce Kss (AV information) is less than one week from generating of the enciphering key KcOr it judges whether it is inside of restricted frequencyand if it is less than inside of less than one week or restricted frequencyit is good though the enciphering key Kc corresponding to Kss (AV information) which it is going to reproduce is acquirable from KcFIFO9. Thereforein this case in this invention of claim 8. As a scramble meansas the record scramble means 7 and an enciphering key generating means. MUX12 will correspond as the correspondence relevant information creating means 11 and a recording device as the key encoding means 10 and a correspondence relevant information creating means as KcFIFO9 and a key encoding means as the 2nd key generating means 8 and a storing meansrespectively. In this invention of claim 12the reproduction descrambling means 17 will correspond as the key decoding means 16 and a releasing scramble means as the enciphering key acquisition means 14 and a key encryption decoding means as an enciphering key acquisition meansrespectively.

[0083]In Embodiment 1 mentioned abovethe 1st key generating means 6 presupposed that the record scramble key Kss for carrying out the scramble of the AV information which the record scramble means 7 inputted is generated. Howeveras shown in drawing 4the recording device of this invention is not provided with the 1st key generating means 6but the record scramble means 7The broadcast scramble key Ks sent is inputted via the broadcast descrambling means 5 from a broadcasting stationand it is the broadcast scramble key Ksor is what processed the broadcast scramble key Ksand it is good though the scramble of the AV information is carried out. In that casefrom the record scramble means 7the key encoding means 10 inputs the broadcast scramble key Ks or the thing which processed the broadcast scramble key Ksand enciphers it with the enciphering key Kc.

[0084]In Embodiment 1 mentioned abovethe record scramble means 7 presupposed that the scramble of the AV information is carried out with the record scramble key Kss from the 1st key generating means 6. Howeveras shown in drawing 5the recording device of this invention is not provided with the 1st key generating means 6 and the key encoding means 10but the record scramble means 7It is goodthough the enciphering key Kc from the 2nd key generating means 8 is inputted via KcFIFO9the enciphering key Kc is used as the record scramble key Kc and the scramble of the AV information is carried out with the record scramble key Kc. In this casethe AV information by which scramble was carried out with the record scramble key Kci.e.Kc(AV information)and the record scramble key Kc are recorded on the videotape 20. In that casethe playback equipment of this invention will be provided with the key decoding means 16as shown in drawing 5. Thereforewhen it is going to reproduce Kc (AV information)the scramble key acquisition means 23 specifies the corresponding record scramble key Kcand acquires it out of KcFIFO9. And while the playback descrambling means 17 inputs Kc (AV information) from the videotape 20 via 2nd DMUX13The record scramble

key Kc from the scramble key acquisition means 23 is inputted via the Kc latch means 15 and Kc (AV information) is descrambled with the record scramble key Kc. Therefore by this invention of claims 15 and 20 in this case that is, 1st DMUX2 will correspond as the correspondence relevant information creating means 11 and a recording device as the record scramble means 7 and a correspondence relevant information creating means as KcFIFO9 and a scramble means as the 2nd key generating means 8 and a storing means as a scramble key generating means respectively. In this invention of claims 19 and 22 the reproduction descrambling means 17 will correspond as the scramble key acquisition means 23 and a releasing scramble means as a scramble key acquisition means respectively.

[0085] The recording device of Embodiment 1 mentioned above is provided with the charging means 24 as shown in drawing 6. A user is burdened with the predetermined fee collection to the record when recording Kss (AV information) on the videotape 20. When a predetermined fee is beforehand paid to a broadcasting station etc. by the user or only when recording at least and a predetermined fee is paid though Kss (AV information) is recorded on the videotape 20 it is good. Even if it is not arranged at the position shown in drawing 6 though the charging means 24 is arranged between the key encoding means 10 and MUX12 it is good. What burdens a user with the predetermined fee collection to the record in short when the charging means 24 records Kss (AV information) on the videotape 20 -- it is even -- What is necessary is just to carry out. may an arrangement place be any place?

[0086] Although it presupposed that it will be discarded if each enciphering key Kc passes for one week since generating in Embodiment 1 mentioned above the time discarded may not be limited after one-week progress from generating and may be after [one day] progress may be after [three day] progress or may be after 12-hour progress. lapse of period predetermined [from generating] in short in each enciphering key Kc -- if it carries out it will discard -- even having -- what is necessary is just to carry out

[0087] In Embodiment 1 mentioned above although the enciphering key Kc in which one differs at a time is generated every day even if it is the same day though the 2nd key generating means 8 generates the enciphering key Kc different every several hours it is good. [of the 2nd key generating means 8] It is good though the enciphering key Kc is generated whenever it records Kss (AV information) of a predetermined program on the videotape 20. That is it is good though the enciphering key Kc is generated for every end of the recording from one recording start each time. In short the 2nd key generating means 8 has only to generate the enciphering key Kc for enciphering the record scramble key Kss of Kss (AV information) which it is going to record.

[0088] Although the date information at the time of the enciphering key Kc being generated was used as correspondence relevant information of this invention in Embodiment 1 mentioned above the time as which as for the correspondence relevant information of this invention the record scramble means 7 inputted AV information The time to which the record scramble means 7 carried out the

scramble of the AV information with the record scramble key KssThe time at which the 2nd key generating means 8 generated the enciphering key Kc the time in which Kc FIFO9 stored the enciphering key Kc It may be the information on the time as which the key encoding means 10 enciphered the record scramble key Kss with the enciphering key Kc or the time at which MUX12 recorded Kss (AV information) on the videotape 20. Or it may be the information on the time at the time of the enciphering key Kc mentioned above being generated the time as which the record scramble means 7 inputted AV information etc. and the time which is going to reproduce AV information. In that case based on each enciphering key Kc of the enciphering key Kc list of drawing 2 lowering ranking every day the difference of two time will be taken into consideration and the enciphering key Kc will be acquired. Or time at the time of the enciphering key Kc which the correspondence relevant information of this invention mentioned above being generated time as which the record scramble means 7 inputted AV information etc. Based on the time which is going to reproduce AV information it may be the number information etc. of the enciphering key Kc list of drawing 2 in which it was taken into consideration that each enciphering key Kc of the enciphering key Kc list of drawing 2 lowers ranking every day.

[0089] In Embodiment 1 mentioned above although the videotape 20 as a recording medium was used a recording medium may be not only the videotape 20 but a hard disk.

[0090] Although the record scramble key Kss for the 1st key generating means 6 to carry out the scramble of the AV information is generated in Embodiment 1 mentioned above though the record scramble key Kss is updated in short periodssuch as tens of secondsso that it cannot decode easily for example it is good.

[0091] The recording device or playback equipment mentioned above The predetermined period of one week passes since generating of the enciphering key Kc and when Kss (AV information) corresponding to the enciphering key Kc is not once reproduced before the enciphering key Kc is discarded or use becomes improper it may have a means to notify a user of information to that effect.

[0092]

[Effect of the Invention] This invention can record AV information on a recording medium and can provide the recording device and playback equipment which observe during the effective regeneration phase of the AV information and restriction of effective reproduction frequency so that clearly from the place explained above.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] The block diagram of the recording device of the embodiment of the invention 1 and playback equipment

[Drawing 2]The figure showing an example of the enciphering key Kc list used for the recording device and playback equipment of the embodiment of the invention 1

[Drawing 3]A different block diagram of the recording device of this inventionand playback equipment from drawing 1

[Drawing 4]A block diagram of the recording device of this inventionand playback equipment which is different in drawing 1 or 3

[Drawing 5]The block diagram of the recording device of drawing 1 and this invention which is different in 3 or 4and playback equipment

[Drawing 6]The block diagram of the recording device of drawing 1 and this invention which is different in 34or 5and playback equipment

[Drawing 7]The block diagram of conventional recording playback equipment

[Description of Notations]

- 1 Receiving demodulation means
 - 2 The 1st DMUX
 - 3 EMM decoding means
 - 4 ECM decoding means
 - 5 Broadcast descrambling means
 - 6 The 1st key generating means
 - 7 Record scramble means
 - 8 The 2nd key generating means
 - 9 KcFIFO
 - 10 Key encoding means
 - 11 Correspondence relevant information creating means
 - 12 MUX
 - 13 The 2nd DMUX
 - 14 Enciphering key acquisition means
 - 15 Kc latch means
 - 16 Key decoding means
 - 17 Reproduction descrambling means
 - 18 Video decoder
 - 19 Sound decoder
 - 20 Videotape
 - 21 Display
 - 22 Counter
 - 23 Scramble key acquisition means
 - 24 Charging means
-

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-232776

(43) 公開日 平成11年(1999) 8月27日

(51) Int.Cl.⁶ 識別記号

G 1 1 B 20/10

G 0 9 C 1/00

G 1 1 B 20/00

H 0 4 L 9/08

H 0 4 N 5/91

6 6 0

F I

G 1 1 B 20/10

G 0 9 C 1/00

G 1 1 B 20/00

H 0 4 L 9/00

H 0 4 N 5/91

H

6 6 0 D

Z

6 0 1 Z

P

審査請求 未請求 請求項の数27 O L (全 16 頁) 最終頁に続く

(21) 出願番号 特願平10-27572

(22) 出願日 平成10年(1998) 2月9日

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 山田 正純

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72) 発明者 飯塚 裕之

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72) 発明者 武知 秀明

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(74) 代理人 弁理士 松田 正道

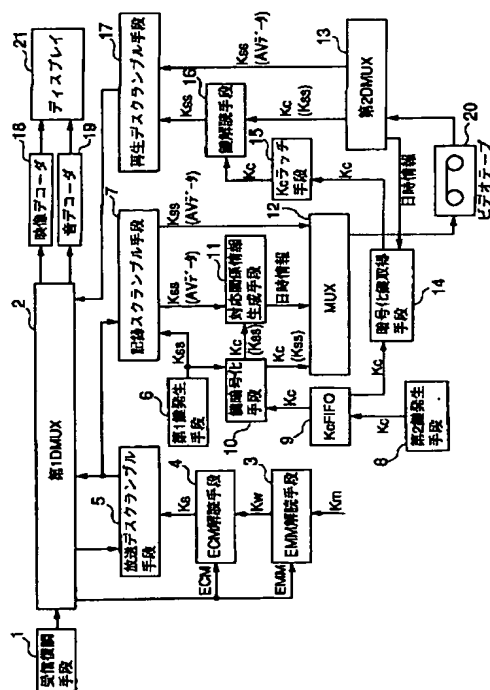
最終頁に続く

(54) 【発明の名称】 録画装置および再生装置

(57) 【要約】

【課題】従来の録画再生装置は、AVデータを記録媒体に記録すると、そのAVデータの有効再生期間や有効再生回数の制限を守らないという課題があった。

【解決手段】スクランブル鍵KssでAVデータをスクランブルする記録スクランブル手段7と、スクランブル鍵Kssを暗号化するための暗号化鍵Kcを発生する第2鍵発生手段8と、第2鍵発生手段8からの暗号化鍵Kcを格納し、その後、その暗号化鍵Kcが所定の条件に合えば、その暗号化鍵Kcを消去するKcFIFO9と、暗号化鍵Kcでスクランブル鍵Kssを暗号化する鍵暗号化手段10と、暗号化鍵Kcが発生された日時の情報を生成する対応関係情報生成手段11と、スクランブルされた映像および／または音のデータ、暗号化されたスクランブル鍵Kss、および、日時情報を入力し、それらをビデオテープ20に記録するMUX12とを備える。



【特許請求の範囲】

【請求項 1】映像および／または音のデータを入力するとともに、前記映像および／または音のデータをスクランブルするためのスクランブル鍵を入力し、そのスクランブル鍵で前記映像および／または音のデータをスクランブルするスクランブル手段と、
前記スクランブル鍵を暗号化するための暗号化鍵を発生する暗号化鍵発生手段と、
前記暗号化鍵発生手段が発生した暗号化鍵を格納し、その後、その暗号化鍵が所定の条件に合えば、その暗号化鍵を消去する格納手段と、
前記スクランブル手段からのスクランブル鍵を入力するとともに、前記暗号化鍵発生手段からの前記暗号化鍵を入力し、その暗号化鍵で前記スクランブル鍵を暗号化する鍵暗号化手段と、
前記スクランブル鍵によりスクランブルされた映像および／または音のデータと、そのスクランブル鍵を暗号化した暗号化鍵との対応関係情報を生成する対応関係情報生成手段と、
前記スクランブル手段からのスクランブルされた映像および／または音のデータ、前記鍵暗号化手段からの暗号化されたスクランブル鍵、および、前記対応関係情報生成手段からの対応関係情報の全部または一部を入力し、それらを所定の記録媒体に記録する記録手段とを備えたことを特徴とする録画装置。

【請求項 2】前記所定の条件とは、前記暗号化鍵が格納された後、所定の時間を超えることを意味することを特徴とする請求項 1 記載の録画装置。

【請求項 3】前記対応関係情報とは、前記スクランブル手段が前記映像および／または音のデータを入力した日時、前記スクランブル手段が前記スクランブル鍵で前記映像および／または音のデータをスクランブルした日時、前記暗号化鍵発生手段が前記暗号化鍵を発生した日時、前記格納手段が前記暗号化鍵を格納した日時、前記鍵暗号化手段が前記暗号化鍵で前記スクランブル鍵を暗号化した日時、または、前記記録手段が前記所定の記録媒体に前記スクランブルされた映像および／または音のデータを記録した日時で対応付けられた情報であることを特徴とする請求項 1 または 2 記載の録画装置。

【請求項 4】前記所定の条件とは、前記スクランブルされた映像および／または音のデータの再生のさいに、前記暗号化鍵の利用された回数が、所定の回数を超えることを意味することを特徴とする請求項 1 記載の録画装置。

【請求項 5】前記スクランブル鍵を発生するスクランブル鍵発生手段を備え、前記スクランブル手段は、前記スクランブル鍵発生手段から前記スクランブル鍵を入力することを特徴とする請求項 1 から 4 のいずれかに記載の録画装置。

【請求項 6】前記スクランブル手段は、放送局からの前

記スクランブル鍵を入力し、そのスクランブル鍵を利用することを特徴とする請求項 1 から 4 のいずれかに記載の録画装置。

【請求項 7】請求項 1 から 6 のいずれかに記載の所定の記録媒体からの、請求項 1 から 6 のいずれかに記載の前記対応関係情報を入力し、その対応関係情報に基づいて、再生しようとするスクランブルされた映像および／または音のデータに対応する暗号化鍵を特定し、請求項 1 から 6 のいずれかに記載の格納手段のなかの前記暗号化鍵を検索して取得する暗号化鍵取得手段と、
前記所定の記録媒体からの、前記再生しようとするスクランブルされた映像および／または音のデータに対応する、暗号化されたスクランブル鍵を入力するとともに、前記暗号化鍵取得手段からの暗号化鍵を入力し、その暗号化鍵で前記暗号化された前記スクランブル鍵の暗号化を解く鍵暗号化読手段と、

前記所定の記録媒体からの、スクランブルされた映像および／または音のデータを入力するとともに、前記鍵暗号化読手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記スクランブルされた映像および／または音のデータのスクランブルを解除するスクランブル解除手段とを備えたことを特徴とする再生装置。

【請求項 8】映像および／または音のデータを入力するとともに、前記映像および／または音のデータをスクランブルするためのスクランブル鍵を入力し、そのスクランブル鍵で前記映像および／または音のデータをスクランブルするスクランブル手段と、

前記スクランブル鍵を暗号化するための暗号化鍵を発生する暗号化鍵発生手段と、

前記暗号化鍵発生手段が発生した暗号化鍵を格納する格納手段と、

前記スクランブル手段からのスクランブル鍵を入力するとともに、前記暗号化鍵発生手段からの前記暗号化鍵を入力し、その暗号化鍵で前記スクランブル鍵を暗号化する鍵暗号化手段と、

前記スクランブル鍵によりスクランブルされた映像および／または音のデータと、そのスクランブル鍵を暗号化した暗号化鍵との対応関係情報を生成する対応関係情報生成手段と、

前記スクランブル手段からのスクランブルされた映像および／または音のデータ、前記鍵暗号化手段からの暗号化されたスクランブル鍵、および、前記対応関係情報生成手段からの対応関係情報の全部または一部を入力し、それらを所定の記録媒体に記録する記録手段とを備えたことを特徴とする録画装置。

【請求項 9】前記対応関係情報とは、前記スクランブル手段が前記映像および／または音のデータを入力した日時、前記スクランブル手段が前記スクランブル鍵で前記映像および／または音のデータをスクランブルした日時、前記暗号化鍵発生手段が前記暗号化鍵を発生した日

時、前記格納手段が前記暗号化鍵を格納した日時、前記鍵暗号化手段が前記暗号化鍵で前記スクランブル鍵を暗号化した日時、または、前記記録手段が前記所定の記録媒体に前記スクランブルされた映像および／または音のデータを記録した日時で対応付けられた情報であることを特徴とする請求項 8 記載の録画装置。

【請求項 1 0】前記スクランブル鍵を発生するスクランブル鍵発生手段を備え、前記スクランブル手段は、前記スクランブル鍵発生手段から前記スクランブル鍵を入力することを特徴とする請求項 8 または 9 記載の録画装置。

【請求項 1 1】前記スクランブル手段は、放送局からの前記スクランブル鍵を入力し、そのスクランブル鍵を利用することを特徴とする請求項 8 または 9 記載の録画装置。

【請求項 1 2】請求項 8 から 1 1 のいずれかに記載の所定の記録媒体からの、請求項 8 から 1 1 のいずれかに記載の対応関係情報を入力し、その対応関係情報に基づいて、再生しようとするスクランブルされた映像および／または音のデータに対応する暗号化鍵を特定し、さらに、その暗号化鍵が所定の条件に合うかどうかを判定し、合致する場合は、その暗号化鍵を、請求項 8 から 1 1 のいずれかに記載の格納手段から取り出し、合致しない場合は、その暗号化鍵を前記格納手段から取り出さない暗号化鍵取得手段と、

前記所定の記録媒体からの、前記再生しようとするスクランブルされた映像および／または音のデータに対応する、暗号化されたスクランブル鍵を入力するとともに、前記暗号化鍵取得手段からの暗号化鍵を入力し、その暗号化鍵で前記暗号化された前記スクランブル鍵の暗号化を解く鍵暗号化読手段と、

前記所定の記録媒体からの、スクランブルされた映像および／または音のデータを入力するとともに、前記鍵暗号化読手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記スクランブルされた映像および／または音のデータのスクランブルを解除するスクランブル解除手段とを備えたことを特徴とする再生装置。

【請求項 1 3】前記所定の条件とは、請求項 8 から 1 1 のいずれかに記載の格納手段に、前記暗号化鍵が格納された後、所定の時間を超えることを意味することを特徴とする請求項 1 2 記載の再生装置。

【請求項 1 4】前記所定の条件とは、前記スクランブルされた映像および／または音のデータの再生のさいに、前記暗号化鍵の利用された回数が、所定の回数を超えることを意味することを特徴とする請求項 1 2 記載の再生装置。

【請求項 1 5】映像および／または音のデータをスクランブルするためのスクランブル鍵を発生するスクランブル鍵発生手段と、
前記スクランブル鍵発生手段が発生したスクランブル鍵

を格納し、その後、そのスクランブル鍵が所定の条件に合えば、そのスクランブル鍵を消去する格納手段と、
前記映像および／または音のデータを入力するとともに、前記スクランブル鍵発生手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記映像および／または音のデータをスクランブルするスクランブル手段と、
前記スクランブル鍵によりスクランブルされた映像および／または音のデータと、そのスクランブル鍵との対応関係情報を生成する対応関係情報生成手段と、
前記スクランブル手段からのスクランブルされた映像および／または音のデータ、および、前記対応関係情報生成手段からの対応関係情報の全部または一部を入力し、それらを所定の記録媒体に記録する記録手段とを備えたことを特徴とする録画装置。

【請求項 1 6】前記所定の条件とは、前記スクランブル鍵が格納された後、所定の時間を超えることを意味することを特徴とする請求項 1 5 記載の録画装置。

【請求項 1 7】前記対応関係情報とは、前記スクランブル手段が前記映像および／または音のデータを入力した日時、前記スクランブル手段が前記スクランブル鍵で前記映像および／または音のデータをスクランブルした日時、前記スクランブル鍵発生手段が前記スクランブル鍵を発生した日時、前記格納手段が前記スクランブル鍵を格納した日時、または、前記記録手段が前記所定の記録媒体に前記スクランブルされた映像および／または音のデータを記録した日時で対応付けられた情報であることを特徴とする請求項 1 5 または 1 6 記載の録画装置。

【請求項 1 8】前記所定の条件とは、前記スクランブルされた映像および／または音のデータの再生のさいに、前記暗号化鍵の利用された回数が、所定の回数を超えることを意味することを特徴とする請求項 1 5 記載の録画装置。

【請求項 1 9】請求項 1 5 から 1 8 のいずれかに記載の所定の記録媒体からの、請求項 1 5 から 1 8 のいずれかに記載の対応関係情報を入力し、その対応関係情報に基づいて、再生しようとするスクランブルされた映像および／または音のデータに対応するスクランブル鍵を特定し、請求項 1 5 から 1 8 のいずれかに記載の格納手段のなかの前記スクランブル鍵を検索して取得するスクランブル鍵取得手段と、

前記所定の記録媒体からの、前記再生しようとするスクランブルされた映像および／または音のデータに対応する、前記スクランブルされた映像および／または音のデータを入力するとともに、前記スクランブル鍵取得手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記スクランブルされた映像および／または音のデータのスクランブルを解除するスクランブル解除手段とを備えたことを特徴とする再生装置。

【請求項 2 0】映像および／または音のデータをスクランブルするためのスクランブル鍵を発生するスクランブル

ル鍵発生手段と、
前記スクランブル鍵発生手段が発生したスクランブル鍵を格納する格納手段と、
前記映像および／または音のデータを入力するとともに、前記スクランブル鍵発生手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記映像および／または音のデータをスクランブルするスクランブル手段と、
前記スクランブル鍵によりスクランブルされた映像および／または音のデータと、そのスクランブル鍵との対応関係情報を生成する対応関係情報生成手段と、
前記スクランブル手段からのスクランブルされた映像および／または音のデータ、および、前記対応関係情報生成手段からの対応関係情報の全部または一部を入力し、それらを所定の記録媒体に記録する記録手段とを備えたことを特徴とする録画装置。

【請求項 2 1】前記対応関係情報とは、前記スクランブル手段が前記映像および／または音のデータを入力した日時、前記スクランブル手段が前記スクランブル鍵で前記映像および／または音のデータをスクランブルした日時、前記スクランブル鍵発生手段が前記スクランブル鍵を発生した日時、前記格納手段が前記スクランブル鍵を格納した日時、または、前記記録手段が前記所定の記録媒体に前記スクランブルされた映像および／または音のデータを記録した日時で対応付けられた情報であることを特徴とする請求項 2 0 記載の録画装置。

【請求項 2 2】請求項 2 0 または 2 1 記載の所定の記録媒体からの、請求項 2 0 または 2 1 記載の対応関係情報を入力し、その対応関係情報に基づいて、再生しようとするスクランブルされた映像および／または音のデータに対応するスクランブル鍵を特定し、さらに、そのスクランブル鍵が所定の条件に合うかどうかを判定し、合致する場合は、そのスクランブル鍵を、請求項 2 0 または 2 1 記載の格納手段から取り出し、合致しない場合は、そのスクランブル鍵を前記格納手段から取り出さないスクランブル鍵取得手段と、

前記所定の記録媒体からの、前記再生しようとするスクランブルされた映像および／または音のデータに対応する、スクランブルされた映像および／または音のデータを入力するとともに、前記スクランブル鍵取得手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記スクランブルされた映像および／または音のデータのスクランブルを解除するスクランブル解除手段とを備えたことを特徴とする再生装置。

【請求項 2 3】前記所定の条件とは、請求項 2 0 または 2 1 記載の格納手段に、前記スクランブル鍵が格納された後、所定の時間を超えることを意味することを特徴とする請求項 2 2 記載の再生装置。

【請求項 2 4】前記所定の条件とは、前記スクランブルされた映像および／または音のデータの再生のさいに、前記スクランブル鍵の利用された回数が、所定の回数を

超えることを意味することを特徴とする請求項 2 2 記載の再生装置。

【請求項 2 5】前記記録手段が前記スクランブル手段からのスクランブルされた映像および／または音のデータを、前記所定の記録媒体に記録するさい、前記データの記録に対する課金を課す課金手段を備えたことを特徴とする請求項 1 から 6 のいずれか、または、請求項 8 から 1 1 のいずれか、または、請求項 1 5 から 1 8 のいずれか、または、請求項 2 0 から 2 1 のいずれかに記載の録画装置。

【請求項 2 6】前記所定の記録媒体は、ビデオテープであることを特徴とする請求項 1 から 6 のいずれか、または、請求項 8 から 1 1 のいずれか、または、請求項 1 5 から 1 8 のいずれか、または、請求項 2 0 から 2 1 のいずれかに記載の録画装置。

【請求項 2 7】前記所定の記録媒体は、ハードディスクであることを特徴とする請求項 1 から 6 のいずれか、または、請求項 8 から 1 1 のいずれか、または、請求項 1 5 から 1 8 のいずれか、または、請求項 2 0 から 2 1 のいずれかに記載の録画装置。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】本発明は、著作権等により再生についての期間や回数が制限された、映像および／または音のデータを録画する録画装置と、その映像および／または音のデータを再生する再生装置とに関するものである。

【0 0 0 2】

【従来の技術】現在、著作権保護の対象となっている映画や音楽等の A V データは、ビデオテープ等に格納されている。ユーザは、そのようなビデオテープ等を有料で貸し出すレンタル店を通じて、例えば 1 週間というような所定の期間のみビデオテープ等を借り、それを再生することによって、映画や音楽等を鑑賞することができる。

【0 0 0 3】他方、上述したビデオテープ等のレンタルのシステムとは別に、デジタル技術や暗号化技術の進歩等から、放送局からの映画や音楽等の番組を通信衛星を介して入力し、その番組をスクランブルしてビデオテープ等に録画し、再生する録画再生装置として、以下のものが考えられている。

【0 0 0 4】図 7 に、このような従来の録画再生装置のブロック図を示す。

【0 0 0 5】受信復調手段 1 は、衛星放送の、デジタルの映像データ、音データ、E M M (個別情報)、E C M (番組情報) および暗号化された放送スクランブル鍵 K s を入力し、第 1 D M U X 2 は、受信復調手段 1 からの映像データ、音データ、E M M、E C M および放送スクランブル鍵 K s を分離する。そして、E M M 解読手段 3 は、第 1 D M U X 2 からの E M M を入力するとともに

に、ユーザID鍵Kmを入力し、そのユーザID鍵KmでEMMを解読してワーク鍵Kwを生成する。ECM解読手段4は、EMM解読手段3からのワーク鍵Kwを入力するとともに、第1DMUX2からのECMおよび暗号化された放送スクランブル鍵Ksを入力し、ワーク鍵KwでECMを解読して、暗号化された放送スクランブル鍵Ksを復元する。

【0006】その後、放送デスクランブル手段5は、ECM解読手段4からの放送スクランブル鍵Ksを入力するとともに、第1DMUX2からの、スクランブルされたAVデータを入力し、放送スクランブル鍵Ksで、スクランブルされたAVデータをデスクランブルする。そして、放送デスクランブル手段5は、デスクランブルされたAVデータを、リアルタイムでAVデータを直接ディスプレイ21に表示させる場合に第1DMUX2に出力し、また、ビデオテープ20にAVデータを記録させる場合に記録スクランブル手段7に出力する。

【0007】放送デスクランブル手段5がAVデータを第1DMUX2に出力する場合、第1DMUX2は、放送デスクランブル手段5からのAVデータを映像データと音データに分離して、映像データを映像デコーダ18に出力し、音データを音デコーダ19に出力する。そして、映像デコーダ18および音デコーダ19それぞれは、第1DMUX2からの映像データまたは音データを復号し、ディスプレイ21は、映像を表示し音を出力する。

【0008】他方、放送デスクランブル手段5がAVデータを記録スクランブル手段7に出力する場合、記録スクランブル手段7は、放送デスクランブル手段5からのAVデータを入力するとともに、第1鍵発生手段6からの記録スクランブル鍵Kssを入力し、その記録スクランブル鍵Kssで、AVデータをスクランブルする。その記録スクランブル鍵KssによりスクランブルされたAVデータをKss(AVデータ)とする。

【0009】それとともに、第2鍵発生手段8は、記録スクランブル鍵Kssを暗号化するための暗号化鍵Kcを発生し、鍵暗号化手段10は、第1鍵発生手段6からの記録スクランブル鍵Kssを入力するとともに、第2鍵発生手段8からの暗号化鍵Kcを入力し、その暗号化鍵Kcで記録スクランブル鍵Kssを暗号化する。その暗号化鍵Kcにより暗号化された記録スクランブル鍵KssをKc(Kss)とする。

【0010】そして、MUX12は、記録スクランブル手段7からのKss(AVデータ)と、鍵暗号化手段10からのKc(Kss)とを入力し、それらをビデオテープ20に記録する。

【0011】そのビデオテープ20に記録されたKss(AVデータ)を再生する場合、先ず、第2DMUX13は、ビデオテープ20からのKss(AVデータ)と、Kc(Kss)とを入力して分離する。そして、鍵

解読手段16は、第2DMUX13からのKc(Kss)を入力するとともに、第2鍵発生手段8からの暗号化鍵Kcを入力し、その暗号化鍵KcでKc(Kss)を解読して、記録スクランブル鍵Kssを復元する。さらに、再生デスクランブル手段17は、第2DMUX13からのKss(AVデータ)を入力するとともに、鍵解読手段16からの記録スクランブル鍵Kssを入力し、その記録スクランブル鍵KssでKss(AVデータ)をデスクランブルして、そのデスクランブルされたAVデータを第1DMUX2に出力する。

【0012】最後に、第1DMUX2に出力されたAVデータは、リアルタイムにおける、ディスプレイ21の映像表示および音出力と同様に、ディスプレイ21によって映像として表示され、また、音として出力される。

【0013】

【発明が解決しようとする課題】ところで、上述したビデオテープ等のレンタルのシステムは、これからの多チャンネルデジタル放送時代においても、ユーザがその都度レンタル店に出向いてビデオテープ等を借りなければならないという点など、ユーザにとって相変わず手間がかかり不便である。

【0014】また、上述した従来の録画再生装置では、AVデータを一度ビデオテープ20に記録すると、第2鍵発生手段8からの暗号化鍵Kcを利用しさえすれば、そのAVデータは、いつでも、また、何度でも再生され、ディスプレイ21によって映像および／または音として出力される。このように、従来の録画再生装置では、映画や音楽等の著作権保護の対象となっているAVデータの有効再生期間や有効再生回数には制限がないということになる。例えば、劇場放映直後の映画のように、特別な価値を有するAVデータが上述したような、再生の期間や回数について制限のない録画再生装置によって記録媒体に記録されると、そのAVデータの価値は半減する。つまり、放送局は、そのような特別な価値を有するAVデータを安心して放送することができない。

【0015】本発明は、このような従来の録画再生装置は、AVデータを記録媒体に記録すると、そのAVデータの有効再生期間や有効再生回数の制限を守らないという課題を考慮し、AVデータを記録媒体に記録し、そのAVデータの有効再生期間や有効再生回数の制限を遵守する録画装置および再生装置を提供することを目的とするものである。

【0016】

【課題を解決するための手段】請求項1の本発明は、映像および／または音のデータを入力するとともに、前記映像および／または音のデータをスクランブルするためのスクランブル鍵を入力し、そのスクランブル鍵で前記映像および／または音のデータをスクランブルするスクランブル手段と、前記スクランブル鍵を暗号化するため

の暗号化鍵を発生する暗号化鍵発生手段と、前記暗号化鍵発生手段が発生した暗号化鍵を格納し、その後、その暗号化鍵が所定の条件に合えば、その暗号化鍵を消去する格納手段と、前記スクランブル手段からのスクランブル鍵を入力するとともに、前記暗号化鍵発生手段からの前記暗号化鍵を入力し、その暗号化鍵で前記スクランブル鍵を暗号化する鍵暗号化手段と、前記スクランブル鍵によりスクランブルされた映像および／または音のデータと、そのスクランブル鍵を暗号化した暗号化鍵との対応関係情報を生成する対応関係情報生成手段と、前記スクランブル手段からのスクランブルされた映像および／または音のデータ、前記鍵暗号化手段からの暗号化されたスクランブル鍵、および、前記対応関係情報生成手段からの対応関係情報の全部または一部を入力し、それらを所定の記録媒体に記録する記録手段とを備えたことを特徴とする録画装置である。

【0017】請求項7の本発明は、請求項1から6のいずれかに記載の所定の記録媒体からの、請求項1から6のいずれかに記載の前記対応関係情報を入力し、その対応関係情報に基づいて、再生しようとするスクランブルされた映像および／または音のデータに対応する暗号化鍵を特定し、請求項1から6のいずれかに記載の格納手段のなかの前記暗号化鍵を検索して取得する暗号化鍵取得手段と、前記所定の記録媒体からの、前記再生しようとするスクランブルされた映像および／または音のデータに対応する、暗号化されたスクランブル鍵を入力するとともに、前記暗号化鍵取得手段からの暗号化鍵を入力し、その暗号化鍵で前記暗号化された前記スクランブル鍵の暗号化を解く鍵暗号化読手段と、前記所定の記録媒体からの、スクランブルされた映像および／または音のデータを入力するとともに、前記鍵暗号化読手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記スクランブルされた映像および／または音のデータのスクランブルを解除するスクランブル解除手段とを備えたことを特徴とする再生装置である。

【0018】請求項8の本発明は、映像および／または音のデータを入力するとともに、前記映像および／または音のデータをスクランブルするためのスクランブル鍵を入力し、そのスクランブル鍵で前記映像および／または音のデータをスクランブルするスクランブル手段と、前記スクランブル鍵を暗号化するための暗号化鍵を発生する暗号化鍵発生手段と、前記暗号化鍵発生手段が発生した暗号化鍵を格納する格納手段と、前記スクランブル手段からのスクランブル鍵を入力するとともに、前記暗号化鍵発生手段からの前記暗号化鍵を入力し、その暗号化鍵で前記スクランブル鍵を暗号化する鍵暗号化手段と、前記スクランブル鍵によりスクランブルされた映像および／または音のデータと、そのスクランブル鍵を暗号化した暗号化鍵との対応関係情報を生成する対応関係情報生成手段と、前記スクランブル手段からのスクラン

ブルされた映像および／または音のデータ、前記鍵暗号化手段からの暗号化されたスクランブル鍵、および、前記対応関係情報生成手段からの対応関係情報の全部または一部を入力し、それらを所定の記録媒体に記録する記録手段とを備えたことを特徴とする録画装置である。

【0019】請求項12の本発明は、請求項8から11のいずれかに記載の所定の記録媒体からの、請求項8から11のいずれかに記載の対応関係情報を入力し、その対応関係情報に基づいて、再生しようとするスクランブルされた映像および／または音のデータに対応する暗号化鍵を特定し、さらに、その暗号化鍵が所定の条件に合うかどうかを判定し、合致する場合は、その暗号化鍵を、請求項8から11のいずれかに記載の格納手段から取り出し、合致しない場合は、その暗号化鍵を前記格納手段から取り出さない暗号化鍵取得手段と、前記所定の記録媒体からの、前記再生しようとするスクランブルされた映像および／または音のデータに対応する、暗号化されたスクランブル鍵を入力するとともに、前記暗号化鍵取得手段からの暗号化鍵を入力し、その暗号化鍵で前記暗号化された前記スクランブル鍵の暗号化を解く鍵暗号化読手段と、前記所定の記録媒体からの、スクランブルされた映像および／または音のデータを入力するとともに、前記鍵暗号化読手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記スクランブルされた映像および／または音のデータのスクランブルを解除するスクランブル解除手段とを備えたことを特徴とする再生装置である。

【0020】請求項15の本発明は、映像および／または音のデータをスクランブルするためのスクランブル鍵を発生するスクランブル鍵発生手段と、前記スクランブル鍵発生手段が発生したスクランブル鍵を格納し、その後、そのスクランブル鍵が所定の条件に合えば、そのスクランブル鍵を消去する格納手段と、前記映像および／または音のデータを入力するとともに、前記スクランブル鍵発生手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記映像および／または音のデータをスクランブルするスクランブル手段と、前記スクランブル鍵によりスクランブルされた映像および／または音のデータと、そのスクランブル鍵との対応関係情報を生成する対応関係情報生成手段と、前記スクランブル手段からのスクランブルされた映像および／または音のデータ、および、前記対応関係情報生成手段からの対応関係情報の全部または一部を入力し、それらを所定の記録媒体に記録する記録手段とを備えたことを特徴とする録画装置である。

【0021】請求項19の本発明は、請求項15から18のいずれかに記載の所定の記録媒体からの、請求項15から18のいずれかに記載の対応関係情報を入力し、その対応関係情報に基づいて、再生しようとするスクランブルされた映像および／または音のデータに対応する

スクランブル鍵を特定し、請求項 1 5 から 1 8 のいずれかに記載の格納手段のなかの前記スクランブル鍵を検索して取得するスクランブル鍵取得手段と、前記所定の記録媒体からの、前記再生しようとするスクランブルされた映像および／または音のデータに対応する、前記スクランブルされた映像および／または音のデータを入力するとともに、前記スクランブル鍵取得手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記スクランブルされた映像および／または音のデータのスクランブルを解除するスクランブル解除手段とを備えたことを特徴とする再生装置である。

【0022】請求項 2 0 の本発明は、映像および／または音のデータをスクランブルするためのスクランブル鍵を発生するスクランブル鍵発生手段と、前記スクランブル鍵発生手段が発生したスクランブル鍵を格納する格納手段と、前記映像および／または音のデータを入力するとともに、前記スクランブル鍵発生手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記映像および／または音のデータをスクランブルするスクランブル手段と、前記スクランブル鍵によりスクランブルされた映像および／または音のデータと、そのスクランブル鍵との対応関係情報を生成する対応関係情報生成手段と、前記スクランブル手段からのスクランブルされた映像および／または音のデータ、および、前記対応関係情報生成手段からの対応関係情報の全部または一部を入力し、それらを所定の記録媒体に記録する記録手段とを備えたことを特徴とする録画装置である。

【0023】請求項 2 2 の本発明は、請求項 2 0 または 2 1 記載の所定の記録媒体からの、請求項 2 0 または 2 1 記載の対応関係情報を入力し、その対応関係情報に基づいて、再生しようとするスクランブルされた映像および／または音のデータに対応するスクランブル鍵を特定し、さらに、そのスクランブル鍵が所定の条件に合うかどうかを判定し、合致する場合は、そのスクランブル鍵を、請求項 2 0 または 2 1 記載の格納手段から取り出し、合致しない場合は、そのスクランブル鍵を前記格納手段から取り出さないスクランブル鍵取得手段と、前記所定の記録媒体からの、前記再生しようとするスクランブルされた映像および／または音のデータに対応する、スクランブルされた映像および／または音のデータを入力するとともに、前記スクランブル鍵取得手段からのスクランブル鍵を入力し、そのスクランブル鍵で前記スクランブルされた映像および／または音のデータのスクランブルを解除するスクランブル解除手段とを備えたことを特徴とする再生装置である。

【0024】

【発明の実施の形態】以下に、本発明の実施の形態を図面を参照して説明する。

【0025】（実施の形態 1）まず、本発明の実施の形態 1 の録画装置および再生装置の構成を述べる。

【0026】図 1 に、本発明の実施の形態 1 の録画装置および再生装置のブロック図を示す。本発明の実施の形態 1 の録画装置は、第 1 鍵発生手段 6 と、記録スクランブル手段 7 と、第 2 鍵発生手段 8 と、K c F I F O 9 と、鍵暗号化手段 1 0 と、対応関係情報生成手段 1 1 と、M U X 1 2 から構成される。また、本発明の実施の形態 1 の再生装置は、第 2 D M U X 1 3 と、暗号化鍵取得手段 1 4 と、K c ラッチ手段 1 5 と、鍵解読手段 1 6 と、再生デスクランブル手段 1 7 から構成される。なお、図 1 には、受信復調手段 1 と、第 1 D M U X 2 と、E M M 解読手段 3 と、E C M 解読手段 4 と、放送デスクランブル手段 5 と、映像デコーダ 1 8 と、音デコーダ 1 9 も表示する。さらに、記録媒体としてのビデオテープ 2 0 と、映像を表示し、音を出力するディスプレイ 2 1 も表示する。

【0027】受信復調手段 1 は、放送局からの、デジタルの映像データ、音データ、E M M（個別情報）、E C M（番組情報）および暗号化された放送スクランブル鍵 K s を通信衛星を介して入力し、それらの全部または一部の信号波形を整形する手段である。

【0028】なお、受信復調手段 1 が入力する映像データおよび音データは、放送スクランブル鍵 K s によりスクランブルされたデータである。また、以下では、映像データと音データの両方を意味する場合、映像データおよび音データを A V データとする。

【0029】また、受信復調手段 1 が入力する E M M（個別情報）は、後に説明するワーク鍵 K w という鍵を生成するさいに必要な情報である。

【0030】さらに、受信復調手段 1 が入力する E C M（番組情報）は、暗号化された放送スクランブル鍵 K s を復元するさいに必要な情報である。

【0031】さて、第 1 D M U X 2 は、受信復調手段 1 からの、波形整形された映像データ、音データ、E M M、E C M および暗号化された放送スクランブル鍵 K s を分離する手段であるとともに、放送デスクランブル手段 5 からの、デスクランブルされた映像データおよび音データを分離する手段である。また、第 1 D M U X 2 は、再生デスクランブル手段 1 7 からの映像データおよび音データを分離する手段でもある。

【0032】E M M 解読手段 3 は、ユーザ I D 鍵 K m を入力するとともに、第 1 D M U X 2 からの E M M を入力し、ユーザ I D 鍵 K m で E M M を解読してワーク鍵 K w を生成する手段である。

【0033】E C M 解読手段 4 は、E M M 解読手段 3 からのワーク鍵 K w を入力するとともに、第 1 D M U X 2 からの E C M および暗号化された放送スクランブル鍵 K s を入力し、ワーク鍵 K w で E C M を解読して放送スクランブル鍵 K s を復元する手段である。

【0034】放送デスクランブル手段 5 は、E C M 解読手段 4 からの放送スクランブル鍵 K s を入力するととも

に、第1DMUX2からの、スクランブルされたAVデータを入力し、放送スクランブル鍵Ksで、スクランブルされたAVデータをデスクランブルする手段である。

【0035】第1鍵発生手段6は、放送デスクランブル手段5によってデスクランブルされたAVデータを、再度スクランブルするための記録スクランブル鍵Kssを発生する手段である。

【0036】記録スクランブル手段7は、放送デスクランブル手段5からのAVデータを入力するとともに、第1鍵発生手段6からの記録スクランブル鍵Kssを入力し、その記録スクランブル鍵KssでAVデータをスクランブルする手段である。なお、以下では、記録スクランブル鍵KssによりスクランブルされたAVデータをKss(AVデータ)とする。

【0037】第2鍵発生手段8は、第1鍵発生手段6が発生した記録スクランブル鍵Kssを暗号化するための暗号化鍵Kcを発生する手段である。なお、第2鍵発生手段8は、毎日異なる暗号化鍵Kcを発生するものとし、それら異なるKcをそれぞれKc1、Kc2、Kc3、…とする。また、暗号化鍵Kc1、Kc2、Kc3、…それぞれは、1週間で廃棄されるものであるとする。

【0038】KcFIFO9は、第2鍵発生手段8からの暗号化鍵Kc1、Kc2、Kc3、…を入力し格納する手段であるとともに、タイマーを有していて、そのタイマーを利用して、入力後1週間経過した暗号化鍵Kcを廃棄する、ファーストインファースアウト機能を有する手段である。

【0039】鍵暗号化手段10は、第1鍵発生手段6からの記録スクランブル鍵Kssを入力するとともに、KcFIFO9からの暗号化鍵Kcを入力し、その暗号化鍵Kcで記録スクランブル鍵Kssを暗号化する手段である。なお、以下では、暗号化鍵Kcにより暗号化された記録スクランブル鍵KssをKc(Kss)とする。

【0040】対応関係情報生成手段11は、記録スクランブル鍵KssによりスクランブルされたAVデータと、その記録スクランブル鍵Kssを暗号化した暗号化鍵Kcとを対応付けるための情報として、暗号化鍵Kc4が発生された日時の情報を生成する手段である。

【0041】MUX12は、記録スクランブル手段7からのKss(AVデータ)と、鍵暗号化手段10からのKc(Kss)と、対応関係情報生成手段11からの日時情報とを入力し、それらをビデオテープ20に記録する手段である。

【0042】第2DMUX13は、ビデオテープ20に記録された、Kss(AVデータ)、Kc(Kss)および日時情報を入力し、それらを分離する手段である。

【0043】暗号化鍵取得手段14は、第2DMUX13からの日時情報を入力し、その日時情報に基づいて、再生しようとするKss(AVデータ)に対応する暗号

化鍵Kcを特定し、その特定した暗号化鍵KcをKcFIFO9のなかから取得する手段である。

【0044】Kcラッチ手段15は、暗号化鍵取得手段14からの暗号化鍵Kcを入力してラッチし、鍵解読手段16に出力する手段である。

【0045】鍵解読手段16は、第2DMUX13からのKc(Kss)を入力するとともに、Kcラッチ手段15からの暗号化鍵Kcを入力し、その暗号化鍵KcでKc(Kss)を解読し、記録スクランブル鍵Kssを復元する手段である。

【0046】再生デスクランブル手段17は、第2DMUX13からのKss(AVデータ)を入力するとともに、鍵解読手段16からの記録スクランブル鍵Kssを入力し、その記録スクランブル鍵KssでKss(AVデータ)をデスクランブルする手段である。

【0047】映像デコーダ18は、第1DMUX2からの映像データを復号する手段である。

【0048】音デコーダ19は、第1DMUX2からの音データを復号する手段である。

【0049】なお、請求項1の本発明の、スクランブル手段として記録スクランブル手段7、暗号化鍵発生手段として第2鍵発生手段8、格納手段としてKcFIFO9、鍵暗号化手段として鍵暗号化手段10、対応関係情報生成手段として対応関係情報生成手段11、記録手段としてMUX12を用いた。また、請求項6の本発明のスクランブル鍵発生手段として第1鍵発生手段6を、本実施の形態では用いた。さらに、請求項7の本発明の、暗号化鍵取得手段として暗号化鍵取得手段14、鍵暗号化解読手段として鍵解読手段16、スクランブル解除手段として再生デスクランブル手段17を用いた。

【0050】次に、このような本発明の実施の形態1の録画装置の動作を述べる。

【0051】先ず、受信復調手段1は、放送局からの、デジタルの映像データ、音データ、EMM(個別情報)、ECM(番組情報)および暗号化された放送スクランブル鍵Ksを入力し、映像データおよび音データの信号波形の乱れを整形し、映像データ、音データ、EMM、ECMおよび暗号化された放送スクランブル鍵Ksを第1DMUX2に出力する。

【0052】その後、第1DMUX2は、受信復調手段1からの映像データ、音データ、EMM、ECMおよび放送スクランブル鍵Ksを入力して分離し、映像データおよび音データ(AVデータ)を放送デスクランブル手段5に出力する。また、EMMをEMM解読手段3に出力し、ECMおよび暗号化された放送スクランブル鍵KsをECM解読手段4に出力する。

【0053】次に、EMM解読手段3は、ユーザID鍵Kmを入力するとともに、第1DMUX2からのEMMを入力し、ユーザID鍵KmでEMMを解読してワーク鍵Kwを生成し、ECM解読手段4に出力する。

【0054】さらに、ECM解読手段4は、EMM解読手段3からのワーク鍵 K_w を入力するとともに、第1DMUX2からの、ECMおよび暗号化された放送スクランブル鍵 K_s を入力し、ワーク鍵 K_w でECMを解読して、暗号化された放送スクランブル鍵 K_s の暗号化を復元し、放送デスクランブル手段5に出力する。そして、放送デスクランブル手段5は、ECM解読手段4からの放送スクランブル鍵 K_s を入力するとともに、第1DMUX2からの、スクランブルされたAVデータを入力し、放送スクランブル鍵 K_s で、スクランブルされたAVデータをデスクランブルする。そして、放送デスクランブル手段5は、デスクランブルされたAVデータを第1DMUX2または記録スクランブル手段7に出力する。なお、放送デスクランブル手段5は、リアルタイムでAVデータを直接ディスプレイ21に表示させる場合に第1DMUX2に出力し、ビデオテープ20にAVデータを記録させる場合に記録スクランブル手段7に出力する。ただし、ビデオテープ20に記録されるAVデータは、放送デスクランブル手段5からの、そのままのAVデータではなく、再度スクランブルされたデータである。

【0055】はじめに、放送デスクランブル手段5がAVデータを第1DMUX2に出力する場合について説明する。

【0056】その場合、第1DMUX2は、放送デスクランブル手段5からのAVデータ入力し、それを映像データと音データに分離して、映像データを映像デコーダ18に出力し、音データを音デコーダ19に出力する。その後、映像デコーダ18および音デコーダ19それぞれは、第1DMUX2からの映像データまたは音データを復号し、ディスプレイ21に出力する。そして、ディスプレイ21は、映像を表示し音を出力する。

【0057】次に、放送デスクランブル手段5がAVデータを記録スクランブル手段7に出力する場合について説明する。つまり、上述したように、ビデオテープ20にAVデータを記録する場合である。

【0058】まず、記録スクランブル手段7は、放送デスクランブル手段5からの、デスクランブルされたAVデータを入力する。

【0059】そして、第1鍵発生手段6は、記録スクランブル手段7が入力したAVデータをスクランブルするための記録スクランブル鍵 K_{ss} を発生し、記録スクランブル手段7および鍵暗号化手段10に出力する。

【0060】次に、記録スクランブル手段7は、第1鍵発生手段6からの記録スクランブル鍵 K_{ss} を入力し、その記録スクランブル鍵 K_{ss} でAVデータをスクランブルする。つまり、 K_{ss} (AVデータ) を生成する。そして、 K_{ss} (AVデータ) を対応関係情報生成手段11およびMUX12に出力する。

【0061】他方、第2鍵発生手段8は、第1鍵発生手

段6が発生した記録スクランブル鍵 K_{ss} を暗号化するための暗号化鍵 K_c を発生する。その第2鍵発生手段8が発生する暗号化鍵 K_c は毎日異なるものとする。ここでは、以下の説明の便宜上、録画装置が動作し始める日を1998年1月1日であるとし、記録時である本日をその日から3日後の1998年1月4日であるとし、図2の暗号化鍵 K_c リスト(a)に示すように、1月1日に発生された暗号化鍵 K_c を K_{c1} 、1月2日に発生された暗号化鍵 K_c を K_{c2} 、…、1月4日に発生された暗号化鍵 K_c を K_{c4} とする。また、以下、同様にして暗号化鍵 K_c は発生されるものとする。なお、ことわりがない限り、以下、1月4日の録画装置の動作について説明する。

【0062】さて、 K_{cFIFO9} は、図2(a)のリストに示すように、1月1日から毎日一つずつの暗号化鍵 K_c を第2鍵発生手段8から既に入力して格納し、1月3日までに暗号化鍵 K_{c1} 、 K_{c2} 、 K_{c3} を格納しておき、本日1月4日には、 K_{c4} を入力して格納する。その格納は、常に最新の暗号化鍵 K_c が図2(a)のリストのトップの順位にくるように行われ、また、古いものは順次順位を下げるように行われる。なお、 K_{cFIFO9} は、格納した暗号化鍵 K_{c1} 、 K_{c2} 、…を、それぞれの格納から1週間経過した後に廃棄する。例えば、図2(b)のリストに示すように、1月9日になると、 K_{c1} 、 K_{c2} という暗号化鍵は廃棄され、 K_{cFIFO9} は、 K_{c9} 、 K_{c8} 、…、 K_{c4} 、 K_{c3} という順序で7つの暗号化鍵を格納することになる。つまり、 K_{cFIFO9} が格納する暗号化鍵 K_c の数は7までである。

【0063】次に、鍵暗号化手段10は、第1鍵発生手段6からの記録スクランブル鍵 K_{ss} を入力するとともに、 K_{cFIFO9} を介して、第2鍵発生手段8が記録時である1月4日に発生した暗号化鍵 K_{c4} を入力し、その暗号化鍵 K_{c4} で記録スクランブル鍵 K_{ss} を暗号化する。つまり、 K_{c4} (K_{ss}) を生成する。

【0064】そして、対応関係情報生成手段11は、記録スクランブル手段7からの K_{ss} (AVデータ) と、鍵暗号化手段10からの K_{c4} (K_{ss}) とを入力し、その暗号化鍵 K_{c4} と、その暗号化鍵 K_{c4} で暗号化された記録スクランブル鍵 K_{ss} によりスクランブルされたAVデータとを対応付けるための情報として、その暗号化鍵 K_{c4} が発生された日時の情報を生成する。つまり、1月4日という日時情報を生成する。

【0065】その後、MUX12は、記録スクランブル手段7からの K_{ss} (AVデータ) と、鍵暗号化手段10からの K_{c4} (K_{ss}) と、対応関係情報生成手段11からの1月4日という日時情報とを入力し、それらを1組としてビデオテープ20に記録する。

【0066】このようにして、毎日、その日に発生された暗号化鍵 K_{cn} ($n=1, 2, \dots$) に対応する K_{cn}

(Kss)と、Kss(AVデータ)と、その日の日時情報とが1組となってビデオテープ20に記録される。

【0067】次に、本発明の実施の形態1の再生装置の動作を述べる。

【0068】つまり、録画装置によってビデオテープ20に記録されたKss(AVデータ)を再生する場合について説明する。

【0069】以下の説明の便宜上、再生装置がビデオテープ20のKss(AVデータ)を再生する日を1月9日であるとする。そして、再生装置は、1月1日にビデオテープ20に記録されたKss(AVデータ)と、1月3日にビデオテープ20に記録されたKss(AVデータ)とを再生しようとするものとする。

【0070】はじめに、再生装置が1月1日にビデオテープ20に記録されたKss(AVデータ)を再生しようとする場合について説明する。

【0071】先ず、第2DMUX13は、ビデオテープ20からの、1月1日に記録されたKss(AVデータ)と、Kc1(Kss)と、1月1日という日時情報とを入力し、それらを分離し、1月1日という日時情報を暗号化鍵取得手段14に出力する。

【0072】そして、暗号化鍵取得手段14は、その1月1日という日時情報を入力し、その日時情報に基づいて、暗号化鍵Kc1を特定し、KcFIFO9が格納している、図2(b)のリストのなかから暗号化鍵Kc1を検索する。しかしながら、その暗号化鍵Kc1は、発生から一週間以上経過しているため、KcFIFO9により廃棄されており、図2(b)のリストのなかには存在しない。したがって、暗号化鍵取得手段14は、暗号化鍵Kc1を取得することができない。その結果、再生デスクランブル手段17は、その暗号化鍵Kc1を間接的に用いてデスクランブルする必要がある、1月1日に記録されたKss(AVデータ)をデスクランブルすることができなくなり、そのAVデータがディスプレイ21に出力されても、解読不能なため、ディスプレイ21は、AVデータ本来の映像および音を出力することができない。

【0073】次に、再生装置が1月3日にビデオテープ20に記録されたKss(AVデータ)を再生しようとする場合について説明する。

【0074】先ず、第2DMUX13は、ビデオテープ20からの、1月3日に記録されたKss(AVデータ)と、Kc3(Kss)と、1月3日という日時情報とを入力し、それらを分離し、1月3日という日時情報を暗号化鍵取得手段14に出力する。

【0075】次に、暗号化鍵取得手段14は、その1月3日という日時情報を入力し、その日時情報に基づいて、暗号化鍵Kc3を特定し、KcFIFO9が格納している、図2(b)のリストのなかから暗号化鍵Kc3を検索してその暗号化鍵Kc3を取得し、それをKcラ

ッチ手段15に出力する。

【0076】その後、Kcラッチ手段15は、暗号化鍵Kc3を入力し、鍵解読手段16に出力する。また、第2DMUX13は、Kc3(Kss)を鍵解読手段16に出力する。

【0077】そして、鍵解読手段16は、第2DMUX13からのKc3(Kss)を入力するとともに、Kcラッチ手段15からの暗号化鍵Kc3を入力し、その暗号化鍵Kc3でKc3(Kss)を解読し、記録スクランブル鍵Kssを復元して、その記録スクランブル鍵Kssを再生デスクランブル手段17に出力する。また、第2DMUX13は、Kss(AVデータ)を鍵解読手段16に出力する。

【0078】次に、再生デスクランブル手段17は、第2DMUX13からのKss(AVデータ)を入力するとともに、鍵解読手段16からの記録スクランブル鍵Kssを入力し、その記録スクランブル鍵KssでKss(AVデータ)をデスクランブルして、そのデスクランブルされたAVデータを第1DMUX2に出力する。

【0079】そして、第1DMUX2は、再生デスクランブル手段17からのAVデータを入力し、それを映像データと音データに分離して、映像データを映像デコーダ18に出力し、音データを音デコーダ19に出力する。その後、映像デコーダ18および音デコーダ19それぞれは、第1DMUX2からの映像データまたは音データを復号し、ディスプレイ21に出力する。そして、ディスプレイ21は、映像を表示し音を出力する。

【0080】このようにして、ビデオテープ20に記録されたKss(AVデータ)それぞれは、記録されてから1週間以内でないと、最終的に、本来の映像および音声として再生されない。

【0081】なお、上述した実施の形態1では、ビデオテープ20に記録されたKss(AVデータ)それぞれは、記録されてから1週間以内であれば再生されるとしたが、1週間以内というような期間の制限ではなく、Kss(AVデータ)それぞれの再生回数を、例えば1回や3回というような制限して、その制限再生回数内ではないと、再生されないとしてもよい。つまり、図3に示すように、本発明の再生装置がカウンタ22を備え、そのカウンタ22が各Kss(AVデータ)の再生回数をチェックし、例えば1回や3回というような制限された再生回数に達した場合、KcFIFO9が、そのKss(AVデータ)に対応する暗号化鍵Kcを廃棄するとしてもよい。また、上述した1週間以内というような期間の制限と再生回数の制限を併用するとしてもよい。

【0082】また、上述した実施の形態1では、KcFIFO9は、格納した暗号化鍵Kcを1週間経過した後に廃棄するとした。しかし、KcFIFO9は、格納した暗号化鍵Kcを1週間経過しても廃棄せずに、格納したままにしておき、暗号化鍵取得手段14が、Kss

(AVデータ)を再生しようとする日が暗号化鍵Kcの発生から1週間以内か否かを判断して、または、制限回数以内か否かを判断して、1週間以内または制限回数以内であれば、再生しようとするKss(AVデータ)に対応する暗号化鍵KcをKcFIFO9から取得できるとしてもよい。したがって、この場合、請求項8の本発明では、スクランブル手段として記録スクランブル手段7、暗号化鍵発生手段として第2鍵発生手段8、格納手段としてKcFIFO9、鍵暗号化手段として鍵暗号化手段10、対応関係情報生成手段として対応関係情報生成手段11、記録手段としてMUX12がそれぞれ該当することになる。また、請求項12の本発明では、暗号化鍵取得手段として暗号化鍵取得手段14、鍵暗号化読手段として鍵読手段16、スクランブル解除手段として再生デスクランブル手段17がそれぞれ該当することになる。

【0083】また、上述した実施の形態1では、第1鍵発生手段6は、記録スクランブル手段7が入力したAVデータをスクランブルするための記録スクランブル鍵Kssを発生するとした。しかし、本発明の録画装置は、図4に示すように、第1鍵発生手段6を備えず、記録スクランブル手段7は、放送局から送られてくる放送スクランブル鍵Ksを、放送デスクランブル手段5を介して入力し、その放送スクランブル鍵Ksで、または、その放送スクランブル鍵Ksを加工したもので、AVデータをスクランブルするとしてもよい。その場合、鍵暗号化手段10は、記録スクランブル手段7から、放送スクランブル鍵Ks、または、その放送スクランブル鍵Ksを加工したものを入力し、それを暗号化鍵Kcで暗号化する。

【0084】また、上述した実施の形態1では、記録スクランブル手段7は、第1鍵発生手段6からの記録スクランブル鍵KssでAVデータをスクランブルするとした。しかし、本発明の録画装置は、図5に示すように、第1鍵発生手段6、鍵暗号化手段10を備えず、記録スクランブル手段7は、第2鍵発生手段8からの暗号化鍵KcをKcFIFO9を介して入力し、その暗号化鍵Kcを記録スクランブル鍵Kcとして使用し、その記録スクランブル鍵Kcにより、AVデータをスクランブルするとしてもよい。この場合、ビデオテープ20には、記録スクランブル鍵KcによりスクランブルされたAVデータ、つまり、Kc(AVデータ)と、記録スクランブル鍵Kcとが記録される。またその場合、本発明の再生装置は、図5に示すように、鍵読手段16を備えないことになる。したがって、Kc(AVデータ)を再生しようとする場合、スクランブル鍵取得手段23は、対応する記録スクランブル鍵Kcを特定し、それをKcFIFO9のなかから取得する。そして、再生デスクランブル手段17は、ビデオテープ20からのKc(AVデータ)を第2DMUX13を介して入力するとともに、ス

クランブル鍵取得手段23からの記録スクランブル鍵KcをKcラッチ手段15を介して入力し、その記録スクランブル鍵KcでKc(AVデータ)をデスクランブルする。そのため、この場合、つまり、請求項15および20の本発明では、スクランブル鍵発生手段として第2鍵発生手段8、格納手段としてKcFIFO9、スクランブル手段として記録スクランブル手段7、対応関係情報生成手段として対応関係情報生成手段11、記録手段として第1DMUX2がそれぞれ該当することになる。また、請求項19および22の本発明では、スクランブル鍵取得手段としてスクランブル鍵取得手段23、スクランブル解除手段として再生デスクランブル手段17がそれぞれ該当することになる。

【0085】また、上述した実施の形態1の録画装置は、図6に示すように、課金手段24を備え、ビデオテープ20にKss(AVデータ)を記録するさい、その記録に対する所定の課金をユーザに課し、あらかじめユーザから所定の料金が放送局等に支払われた場合、もしくは、少なくとも記録するさいに所定の料金が支払われた場合のみ、Kss(AVデータ)はビデオテープ20に記録されるとしてもよい。また、課金手段24は、図6に示す位置に配置されなくとも、鍵暗号化手段10とMUX12との間に配置されるとしてもよい。要するに、課金手段24は、ビデオテープ20にKss(AVデータ)を記録するさい、その記録に対する所定の課金をユーザに課すものでありさえすればよく、配置場所はどの場所であってもよい。

【0086】また、上述した実施の形態1では、暗号化鍵Kcそれぞれは、発生から1週間経過すると廃棄されるとしたが、廃棄される日時は、発生から1週間経過後に限定することではなく、1日経過後であっても、3日経過後であっても、または、12時間経過後であってもよい。要するに、暗号化鍵Kcそれぞれは、発生から所定の期間経過すると廃棄されさえすればよい。

【0087】また、上述した実施の形態1では、第2鍵発生手段8は、毎日、1つづつ異なる暗号化鍵Kcを発生するとしたが、第2鍵発生手段8は、同じ日であっても、数時間毎に異なる暗号化鍵Kcを発生するとしてもよい。さらに、ビデオテープ20に所定の番組のKss(AVデータ)を記録する毎に暗号化鍵Kcを発生するとしてもよい。つまり、一回の録画開始からその録画の終了毎に、その都度、暗号化鍵Kcを発生するとしてもよい。要するに、第2鍵発生手段8は、記録しようとするKss(AVデータ)の記録スクランブル鍵Kssを暗号化するための暗号化鍵Kcを発生しさえすればよい。

【0088】また、上述した実施の形態1では、本発明の対応関係情報として、暗号化鍵Kcが発生されたさいの日時情報を用いたが、本発明の対応関係情報は、記録スクランブル手段7がAVデータを入力した日時、記録

スクランブル手段 7 が記録スクランブル鍵 K_{ss} で AV データをスクランブルした日時、第 2 鍵発生手段 8 が暗号化鍵 K_c を発生した日時、 $K_c F I F O 9$ が暗号化鍵 K_c を格納した日時、鍵暗号化手段 10 が暗号化鍵 K_c で記録スクランブル鍵 K_{ss} を暗号化した日時、または、MUX 12 がビデオテープ 20 に K_{ss} (AV データ) を記録した日時の情報であってもよい。もしくは、上述した暗号化鍵 K_c が発生されたさいの日時や、記録スクランブル手段 7 が AV データを入力した日時等と、AV データを再生しようとする日時との情報であってもよい。その場合、図 2 の暗号化鍵 K_c リストの各暗号化鍵 K_c が毎日順位を下げることに基づいて、また、2 つの日時の差が考慮されて、暗号化鍵 K_c が取得されることになる。または、本発明の対応関係情報は、上述した暗号化鍵 K_c が発生されたさいの日時や、記録スクランブル手段 7 が AV データを入力した日時等と、AV データを再生しようとする日時とに基づき、また、図 2 の暗号化鍵 K_c リストの各暗号化鍵 K_c が毎日順位を下げる事が考慮された、図 2 の暗号化鍵 K_c リストの番号情報等であってもよい。

【0089】また、上述した実施の形態 1 では、記録媒体としてのビデオテープ 20 を用いたが、記録媒体は、ビデオテープ 20 に限らず、ハードディスクであってもよい。

【0090】また、上述した実施の形態 1 では、第 1 鍵発生手段 6 は AV データをスクランブルするための記録スクランブル鍵 K_{ss} を発生するが、その記録スクランブル鍵 K_{ss} は、簡単に解読することができないように、例えば数十秒などの短い期間で更新されるとしてもよい。

【0091】さらに、上述した録画装置または再生装置は、暗号化鍵 K_c の発生から例えば 1 週間という所定の期間を経過するなどして、その暗号化鍵 K_c が廃棄されたり、使用不可になる前に、その暗号化鍵 K_c に対応する K_{ss} (AV データ) が一度も再生されていない場合、その旨の情報をユーザに通知する手段を備えてもよい。

【0092】

【発明の効果】以上説明したところから明らかなように、本発明は、AV データを記録媒体に記録し、その AV データの有効再生期間や有効再生回数の制限を遵守す

る録画装置および再生装置を提供することができる。

【図面の簡単な説明】

【図 1】本発明の実施の形態 1 の録画装置および再生装置のブロック図

【図 2】本発明の実施の形態 1 の録画装置および再生装置に使用される暗号化鍵 K_c リストの一例を示す図

【図 3】図 1 とは異なる本発明の録画装置および再生装置のブロック図

【図 4】図 1 または 3 とは異なる本発明の録画装置および再生装置のブロック図

【図 5】図 1、3 または 4 とは異なる本発明の録画装置および再生装置のブロック図

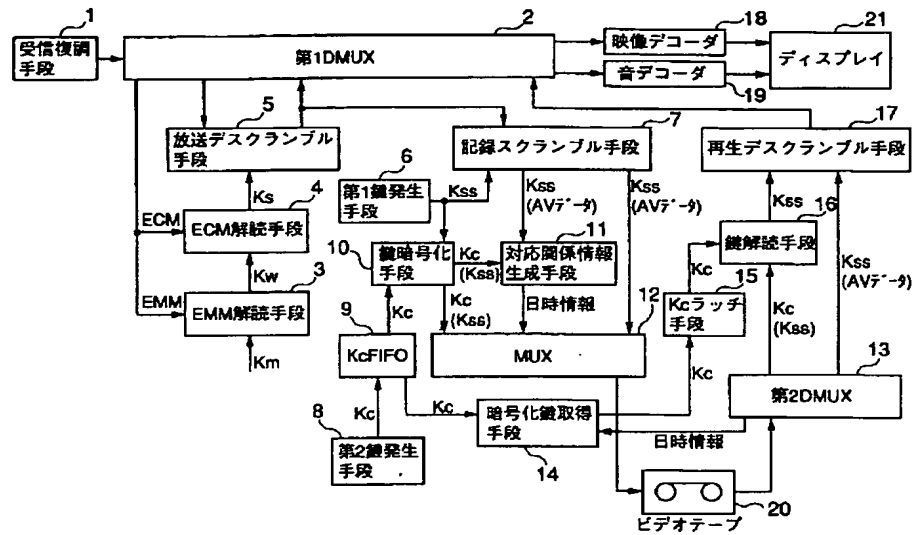
【図 6】図 1、3、4 または 5 とは異なる本発明の録画装置および再生装置のブロック図

【図 7】従来の録画再生装置のブロック図

【符号の説明】

- 1 受信復調手段
- 2 第 1 D M U X
- 3 E M M 解読手段
- 4 E C M 解読手段
- 5 放送デスクランブル手段
- 6 第 1 鍵発生手段
- 7 記録スクランブル手段
- 8 第 2 鍵発生手段
- 9 $K_c F I F O$
- 10 鍵暗号化手段
- 11 対応関係情報生成手段
- 12 M U X
- 13 第 2 D M U X
- 14 暗号化鍵取得手段
- 15 K_c ラッチ手段
- 16 鍵解読手段
- 17 再生デスクランブル手段
- 18 映像デコーダ
- 19 音デコーダ
- 20 ビデオテープ
- 21 ディスプレイ
- 22 カウンタ
- 23 スクランブル鍵取得手段
- 24 課金手段

【図 1】



【図 2】

暗号化鍵 Kc リスト

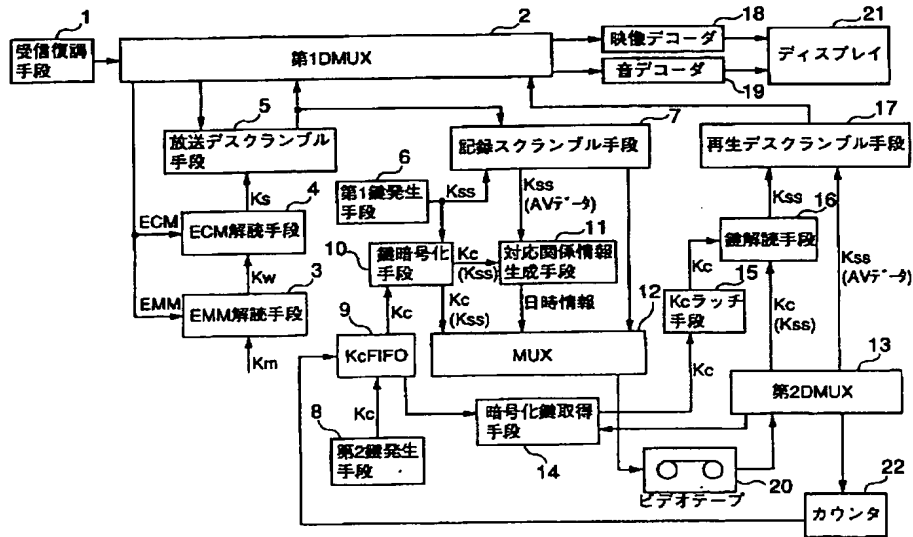
(a) 1月4日 現在

No.	暗号化鍵	鍵発生日
1	Kc 4	1月 4日
2	Kc 3	1月 3日
3	Kc 2	1月 2日
4	Kc 1	1月 1日
5		
6		
7		

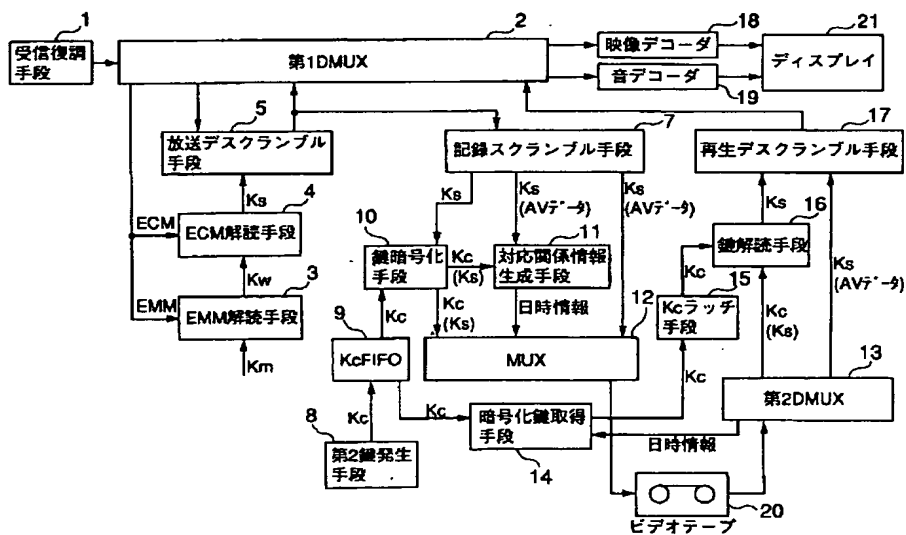
(b) 1月9日 現在

No.	暗号化鍵	鍵発生日
1	Kc 9	1月 9日
2	Kc 8	1月 8日
3	Kc 7	1月 7日
4	Kc 6	1月 6日
5	Kc 5	1月 5日
6	Kc 4	1月 4日
7	Kc 3	1月 3日

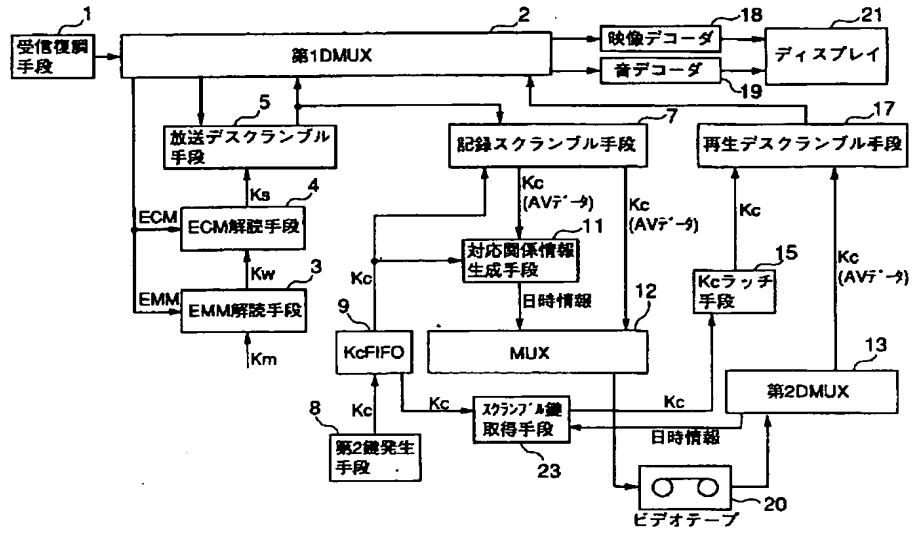
【図 3】



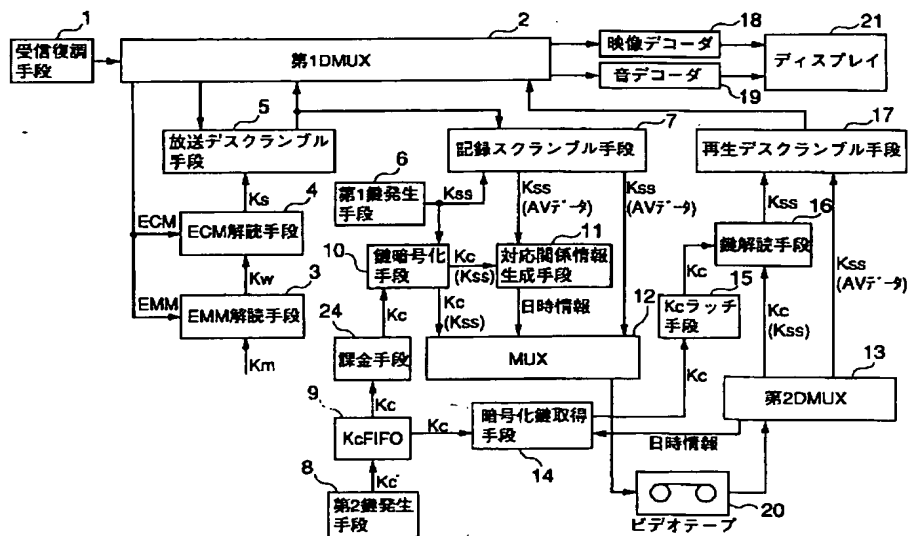
【図 4】



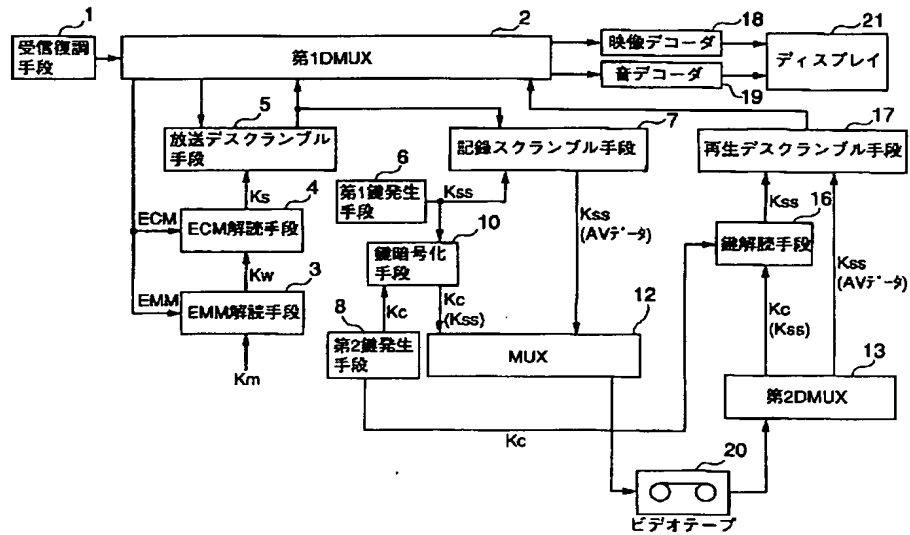
【図5】



【図6】



【図7】



フロントページの続き

(51) Int. Cl. 6

識別記号

F I

H 0 4 N 5/92

H 0 4 N 5/92

Z

// H 0 4 N 7/167

7/167

Z

(72) 発明者 後藤 昌一

大阪府門真市大字門真1006番地 松下電器
産業株式会社内